МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ ІМЕНІ ВАДИМА ГЕТЬМАНА

ІНСТИТУТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ В ЕКОНОМІЦІ

Кафедра системного аналізу та кібербезпеки

ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА «КІБЕРБЕЗПЕКА»

Галузь знань 12 «Інформаційні технології»

Спеціальність 125 «Кібербезпека»

Форма навчання: очна (денна)

КВАЛІФІКАЦІЙНА БАКАЛАВРСЬКА РОБОТА

на тему **«Виявлення вразливостей та розробка рекомендацій по підвищенню рівня кіберзахисту IT інфраструктури для SMB компаній»**

здобувача Щура Олександра Вадимовича _____
(підпис)

Науковий керівник: доктор технічних наук, професор
Толюпа Сергій Васильович

_____
(підпис)

Робота допущена до захисту перед екзаменаційною комісією з атестації здобувачів вищої освіти (ЕК)

Завідувач кафедри: д.ф.-м.н., професор Джалладова І.А.

_____
(підпис)

Київ 2024

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ ІМЕНІ ВАДИМА ГЕТЬМАНА

ІНСТИТУТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ В ЕКОНОМІЦІ

Кафедра системного аналізу та кібербезпеки

ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА «КІБЕРБЕЗПЕКА»

Галузь знань 12 «Інформаційні технології»

Спеціальність 125 «Кібербезпека»

ПОГОДЖЕНО	**ЗАТВЕРДЖУЮ**
Керівник проектної групи (гарант) освітньо-професійної програми «Кібербезпека»	Завідувач кафедри системного анадізу та кібербезпеки
к.ф.-м.н., доцент Г.В. Мамонова	д.ф.-м.н., проф. І.А. Джалладова
2024 р.	2024 р.

ІНДИВІДУАЛЬНЕ ЗАВДАННЯ

здобувача вищої освіти Щура Олександра Вадимовича

денної форми навчання

на підготовку кваліфікаційної бакалаврської роботи

на тему «Виявлення вразливостей та розробка рекомендацій по підвищенню рівня кіберзахисту IT інфраструктури для SMB компаній»

Тему затверджено наказом ректора Університету від 30.04.2024 р. № 726-ст.

Кваліфікаційна бакалаврська робота виконується на матеріалах літературних та інформаційних джерел, моделей побудови та захисту IT інфраструктури, практичної реалізації проекту з аудиту рівня кіберзахисту, виявлення вразливостей та тестування на проникнення IT інфраструктури для типової SMB компанії, а також, вільного доступу до певних ресурсів для побудови графіків та перегляду функціональних можливостей інструментів.

План кваліфікаційної бакалаврської роботи

Розділ 1	Проблематика та аналіз кіберзагроз IT інфраструктури малих та середніх підприємств
Розділ 2	Методи та засоби підвищення рівня кіберзахисту IT інфраструктури
Розділ 3	Виявлення вразливостей та розробка рекомендацій з підвищення рівня кіберзахисту IT інфраструктури для типової SMB компанії

Об'єкт дослідження:	Основні компоненти IT інфраструктури типової SMB компанії
Предмет дослідження:	Методи, інструменти та засоби для виявлення вразливостей та підвищення рівня кіберзахисту
Мета кваліфікаційної бакалаврської роботи:	Виявити вразливості та розробити рекомендації з підвищення рівня кіберзахисту IT інфраструктури типової SMB компанії

Конкретні завдання, які здобувач повинен виконати для досягнення поставленої мети:

У розділі 1 «Проблематика та аналіз кіберзагроз IT інфраструктури малих та середніх підприємств»: розкрити основні компоненти IT інфраструктури та важливість їх своєчасного та системного обслуговування; визначити основні проблеми, типові кіберзагрози та їх наслідки.

У розділі 2 «Методи та засоби підвищення рівня кіберзахисту IT інфраструктури»: визначити та запропонувати відповідні заходи, інструменти, комплекс засобів та дій для підвищення кіберзахисту IT інфраструктури малих та середніх підприємств.

У розділі 3 «Виявлення вразливостей та розробка рекомендацій з підвищення рівня кіберзахисту IT інфраструктури для типової SMB компанії»: на основі практичної реалізації проекту з аудиту рівня кіберзахисту, виявлення вразливостей та тестування на проникнення зовнішнього периметру – розробити план оптимізації та рекомендації щодо усунення виявлених недоліків і вразливостей основних компонентів IT інфраструктури для типової компанії малого та середнього бізнесу.

Завдання підготував
науковий керівник _____ С. В. Толюпа
«_____» _____ 2024 р.

Завдання одержав
здобувач _____ О. В.Щур
«_____» _____ 2024 р.

РЕФЕРАТ

Кваліфікаційна бакалаврська робота містить 3 розділи, 103 сторінки, 11 таблиць, 34 рисунки, список викоритстаних джерел з 42 найменувань.

Об'єкт дослідження: процес підвищення рівня кіберзахисту основних компонентів IT інфраструктури малих та середніх підприємств.

Мета кваліфікаційної роботи: удосконалення, систематизація та підвищення рівня кіберзахисту основних компонентів IT інфраструктури.

Методи дослідження: тестування на проникнення, аудит, аналіз.

В роботі проведено аудит рівня кіберзахисту, виявлення вразливостей та тестування на проникнення, виявлено вразливості та недоліки в організаціїї кіберзахисту.

Запропоновано організаційні та технічні механізми підвищення рівня кіберзахисту основних компонентів IT інфраструктури від типових проблем та кіберзагроз.

Розроблено план оптимізації та рекомендації щодо усунення виявлених недоліків і вразливостей основних компонентів IT інфраструктури для типової компанії малого та середнього бізнесу.

Практичне значення роботи: результати здійснених у кваліфікаційній роботі досліджень можуть бути використані для посилення кіберзахисту основних компонентів IT інфраструктури SMB компаній.

Наукова новизна дослідження: полягає у запропонованих організаційних та технічних механізмах кіберзахисту основних компонентів IT інфраструктури від проникнення та вразливостей.

Напрямком подальших досліджень є удосконалення та уніфікація програмно-апаратних засобів для виявлення вразливостей та посилення кіберзахисту основних компонентів IT інфраструктури компаній малого та середнього бізнесу.

Ключові слова: виявлення вразливостей, тестування на проникнення, кіберзахист, IT інфраструктура, кібергігієна, сканування, фільтрація.

ВІДГУК
на кваліфікаційну бакалаврську роботу
студента Щур Олександра групи ІК-401к
на тему "Виявлення вразливостей та розробка рекомендацій по підвищенню рівня кіберзахисту IT інфраструктури для SMB компаній"

Актуальність теми: У сучасному інформаційному суспільстві кібербезпека стає все більш актуальною. З розвитком технологій та зростанням залежності від них виникають нові загрози, які потребують нових рішень. З розвитком інформаційних технологій та переходом до інформаційного суспільства людство стикається з новими викликами у сфері кібербезпеки. Економіка, міжнародне співробітництво, національна безпека в кіберпросторі та інші сфери життя потребують новітніх систем захисту від кіберзлочинності. Ситуація з кіберзлочинністю потребує постійного удосконалення методів боротьби, розробки нових інформаційних систем та методів для забезпечення кібербезпеки на державному рівні. Таким чином тема є актуальною і потребує детального дослідження.

Повнота розкриття теми: в даній роботі повністю виконані поставлені завдання, її обсяг та зміст відповідає задачам на бакалаврську кваліфікаційну роботу.

Теоретичний рівень: проведене дослідження свідчить про вміння автора опрацьовувати та аналізувати іншомовні видання, нормативні документи, технічну документацію, проводити аналіз, використовувати метод індукції та узагальнювати матеріал.

Практична значимість отриманих результатів полягає у можливості застосування розроблених рекомендацій, інструментів та комплексу дій по виявленню, систематизації, аналізу вразливостей та підвищенню кіберзахисту основних компонентів IT інфраструктури для SMB компаній.

Самостійність виконання роботи: студент показав здатність самостійно працювати з науково-технічною літературою, визначати вектор дослідження, знаходити та обробляти інформацію, має достатні теоретичні знання. Робота відповідає затвердженій темі, а всі етапи, затверджені календарним планом, були виконані у зазначений термін.

Якість оформлення, загальна та спеціальна грамотність: пояснювальна записка кваліфікаційної бакалаврської роботи написана якісно та в доступній для ознайомлення формі.

Переваги та недоліки роботи: кваліфікаційна робота направлена на удосконалення, систематизацію та підвищення рівня кіберзахисту основних компонентів IT інфраструктури типової SMB компанії, що є позитивним.

Загальна оцінка роботи та висновок щодо рекомендації до захисту в ЕК: вважаю, що кваліфікаційна робота виконана на достатньо професійному рівні і студент Щур Олександр підтвердив свою підготовленість до самостійної роботи в галузі інформаційної безпеки, і заслуговує на оцінку

«добре» та присвоєння йому ступеня бакалавра зі спеціальності «Кібербезпека».

Науковий керівник
професор кафедри
системного аналізу та
кібербезпеки ННІ «Інститут
інформаційних технологій в
економіці»
д.т.н., професор _____ С. В. ТОЛЮПА
(підпис) *(ініціали, прізвище)*

«10» червня 2024 р.

РЕЦЕНЗІЯ
на кваліфікаційну бакалаврську роботу
студента Щур Олександра групи ІК-401к
на тему "Виявлення вразливостей та розробка рекомендацій по підвищенню рівня кіберзахисту IT інфраструктури для SMB компаній"

Актуальність теми. Розглянуті в даній роботі проблеми кібербезпеки основних компонентів IT інфраструктури підприємств малого та середнього бізнесу є дуже важливими в зв'язку з тим, що відсутність або недостатньо ефективне та несистемне використання організаційних та технічних механізмів кіберзахисту від проникнення та вразливостей можуть стати слабкою ланкою в підтримці достатнього рівня безпеки і призвести до втрати даних. Тому, кваліфікаційна бакалаврська робота Щура О. В., що присвячена підвищенню рівня безпеки є своєчасною та актуальною.

Наукова новизна роботи полягає в удосконаленню та уніфікації програмно-апаратних засобів для виявлення вразливостей.

Якість проведеного аналізу. Здобувач показав достатньо високий рівень володіння положеннями обраної теми, здатність формувати власну точку зору на основі аналізу наукових робіт різних вчених з цієї галузі та інших джерел інформації.

Вміння користуватися літературними джерелами. В процесі підготовки роботи її автор обробив велику кількість літературних джерел. На високому теоретичному та науковому рівнях проведено дослідження організаційних та технічних механізмів кіберзахисту.

Практична цінність висновків та рекомендацій полягає в тому, що запропоновані рекомендації можуть бути використані для підвищення та посилення рівня кіберзахисту основних компонентів IT інфраструктури SMB компаній.

Переваги та недоліки. Беззаперечною перевагою роботи є проведений практичний аналіз та участь здобувача у проекті з аудиту рівня кібербезпеки IT інфраструктури типової SMB компанії, практична цінність та доступність викладеної інформації. Виявлені деякі не значні недоліки дипломної роботи:

стиль викладення матеріалу не всюди витриманий, недостатньо графіків. Однак це не впливає на якість дослідження даної теми.

Загальний висновок і оцінка роботи. Аналіз запропонованої роботи свідчить про бачення автором цілісної картини проблем кіберзахисту IT інфраструктури малого та середнього бізнесу, що дозволяє зробити висновок про те, що кваліфікаційна бакалаврська робота студента Щура Олександра Вадимовича на тему «Виявлення вразливостей та розробка рекомендацій по підвищенню рівня кіберзахисту IT інфраструктури для SMB компаній» відповідає всім вимогам, що висуваються до кваліфікаційних дипломних робіт. Робота виконана на високому теоретичному, науковому та практичному рівнях і заслуговує оцінки «відмінно», а автору роботи може бути присвоєно освітній рівень «бакалавр» за спеціальністю «Кібербезпека».

Рецензент
Генеральний директор
ПП «ТЕХЕКСПЕРТ»

«18» червня 2024 р.

м. Київ * Україна * Приватне підприємство «ТЕХЕКСПЕРТ» Ідентифікаційний код 39214310

Щур В.П.
(прізвище, ініціали)

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ ТА СКОРОЧЕНЬ

SMB – ринковий сегмент, який становить малий і середній бізнес

ПЗ - програмне забезпечення

ІТ - інформаційні технології

ОС - операційна система

WAN - Wide Area Network глобальна обчислювальна мережа

LAN - Local Area Network - локальна обчислювальна мережа

VM - Virtual Machine - віртуальна машина / віртуальний сервер

DMZ - Demilitarized Zone - демілітаризована зона

VPN - Virtual Private Network - віртуальна приватна мережа

VLAN - Virtual Local Area Network - віртуальна приватна мережа, що дозволяє сегментувати локальну мережу

SSH - мережевий протокол для реалізації шифрованого віддаленого управління і тунелювання трафіку

Core - рівень пристроїв (ядра), забезпечує зв'язок між іншими рівнями мережі

AD - Microsoft Active Directory - служби каталогів корпорації Microsoft для операційних систем сімейства Windows Server

Access - рівень доступу, рівень пристроїв клієнтського доступу

NAT - механізм в мережах TCP / IP, що дозволяє перетворювати IP-адреси транзитних пакетів

HTTP/HTTPS - протокол прикладного рівня передачі даних, HTTPS має шифрування

SNMP - Протокол для управління пристроями в IP-мережах на основі архітектур TCP / UDP

ВСТУП

Актуальність. У сучасному інформаційному суспільстві кібербезпека стає все більш актуальною. З розвитком технологій та зростанням залежності від них виникають нові загрози, які потребують нових рішень. З розвитком інформаційних технологій та переходом до інформаційного суспільства людство стикається з новими викликами у сфері кібербезпеки. Економіка, міжнародне співробітництво, національна безпека в кіберпросторі та інші сфери життя потребують новітніх систем захисту від кіберзлочинності. Ситуація з кіберзлочинністю потребує постійного удосконалення методів боротьби, розробки нових інформаційних систем та методів для забезпечення кібербезпеки на державному рівні.

Війна в Україні стала випробувальним майданчиком для нових ідей та технологій у галузі захисту інформації. Українські кіберфахівці здобувають безцінний досвід, який робить їх лідерами світового ринку. Зростає попит на українські освітні проєкти в цій сфері. Рівень зацікавленості кібербезпекою в українському суспільстві зростає. Елементарними знаннями з кібергігієни повинна володіти кожна людина. Компанії, особливо малого та середнього бізнесу, та їх співробітники повинні приділяти кіберзахисту увагу, навіть якщо це лише кілька хвилин на тиждень. Чим більше суспільство обізнане в питаннях кібербезпеки, тим сильнішою буде наша країна. Україна має потенціал стати лідером у цій сфері та поділитися своїми знаннями зі світом.

Вчені, які зробили значний внесок у розвиток науки кібербезпеки в сучасному світі, зокрема в Україні: Віктор Майєр: американський вчений, який вважається одним із батьків-засновників комп’ютерної безпеки. Розробив модель CIA (Confidentiality, Integrity, Availability) для оцінки ризиків кібербезпеки. Брюс Шнайер: американський криптограф, автор численних книг і статей з кібербезпеки. Розробив алгоритм шифрування Blowfish. Ендрю Таненбаум, голландський вчений, автор операційної системи Minix, яка використовується для навчання з кібербезпеки. Марвін Минський, американський вчений, який зробив значний

внесок у дослідження штучного інтелекту, який зараз використовується в кібербезпеці для виявлення загроз. Томас Салонен, фінський дослідник, який розробив протокол TLS, який використовується для захисту онлайн-з'єднань.

Українські вчені в даній галузі: В. Пилипчук, доктор технічних наук, професор, завідувач кафедри комп'ютерних наук Національного університету «Львівська політехніка», автор понад 200 наукових праць з кібербезпеки; С. Петренко, доктор технічних наук, професор, завідувач кафедри інформаційної безпеки Національного технічного університету України «Київський політехнічний інститут». Автор понад 150 наукових праць з кібербезпеки; Ю. Масютенко, доктор технічних наук, професор, завідувач кафедри комп'ютерних систем і мереж Національного університету «Київський університет імені Тараса Шевченка». Автор понад 100 наукових праць з кібербезпеки; О. Живалова, кандидат технічних наук, доцент кафедри інформаційної безпеки Національного університету оборони України імені Івана Черняховського. Автор понад 50 наукових праць з кібербезпеки; В. Лях, кандидат технічних наук, доцент кафедри комп'ютерних наук Національного педагогічного університету імені Михайла Драгоманова. Автор понад 40 наукових праць з кібербезпеки.

Метою написання кваліфікаційної роботи є удосконалення, систематизація та підвищення рівня кіберзахисту основних компонентів IT інфраструктури типової SMB компанії.

Для досягнення поставленої в роботі мети необхідне вирішення наступних задач:

1. Розглянути основні компоненти IT інфраструктури малих та середніх підприємств, типові кіберзагрози, основні проблеми кіберзахисту.
2. Визначити та запропонувати інструменти, комплекс засобів та дій для підвищення кіберзахисту.
3. Розробити план оптимізації та рекомендації щодо усунення виявлених недоліків і вразливостей основних компонентів IT інфраструктури для типової компанії SMB сегменту.

Об’єктом дослідження роботи є процес підвищення та удосконалення рівня кіберзахисту основних компонентів IT інфраструктури малих та середніх підприємств.

Предметом дослідження роботи є методи, інструменти та засоби для виявлення вразливостей та підвищення рівня кіберзахисту.

Методи дослідження. При написанні роботи було застосовано методи тестування на проникнення, аудиту, аналізу.

Практична значимість отриманих результатів полягає у можливості застосування розроблених рекомендацій, інструментів та комплексу дій по виявленню, систематизації, аналізу вразливостей та підвищенню кіберзахисту основних компонентів IT інфраструктури для SMB компаній.

РОЗДІЛ 1
ПРОБЛЕМАТИКА ТА АНАЛІЗ КІБЕРЗАГРОЗ ІТ ІНФАСТРУКТУРИ МАЛИХ ТА СЕРЕДНІХ ПІДПРИЄМСТВ

1.1 Кібербезпека для малого та середнього бізнесу

У сучасному цифровому світі кібербезпека стає критично важливою для будь-якого бізнесу, незалежно від його розміру. Однак малий та середній бізнес SMB (small-medium business) стикається з унікальними викликами в цій сфері.

SMB більш вразливі, оскільки мають обмежені ресурси: SMB часто не мають бюджету або персоналу для впровадження та підтримки комплексних заходів кібербезпеки. Також це трапляється через нестачу обізнаності: власники та працівники SMB можуть не усвідомлювати серйозності кіберзагроз або не знати, як ефективно захистити свої дані. Немалу роль в цьому відіграють і застарілі системи: SMB частіше використовують застаріле програмне забезпечення та обладнання, яке може бути більш вразливим до кібератак. Також хакери можуть розглядати SMB як легкі цілі, оскільки вони вважають, що у них менш надійні системи захисту.

Кібератаки можуть мати руйнівний вплив на SMB, призводячи до фінансових втрат, а саме викрадення даних, шахрайство та простої можуть призвести до значних фінансових втрат. Також можуть призвести до пошкодження репутації: втрата даних клієнтів або кібератака може серйозно пошкодити репутації SMB і призвести до втрати клієнтів. Як результат таких атак можуть бути неочікувані довгі перерви в роботі: кібератаки можуть призвести до простоїв, що заважає бізнесу функціонувати.

Незважаючи на виклики, SMB можуть вжити низку заходів для захисту від кіберзагроз:

– Створення політики кібербезпеки,

– Навчання персоналу, включаючи те, як розпізнавати та уникати фішингових атак, використовувати надійні паролі та захищати конфіденційні дані,

– Впровадження заходів захисту, антивірусне програмне забезпечення та інші засоби захисту для захисту своїх мереж і систем,

– Регулярне оновлення програмного забезпечення до останніх версій, щоб усунути відомі вразливості,

– Створення резервних копій даних для відновлення їх у разі кібератаки.

– Використання надійних паролів для всіх облікових записів і регулярна їх зміна.

Існують такі особливості товарів та послуг SMB-сегменту:

– Функціональність та універсальність. Рішення пропонують широкий спектр можливостей, які можна адаптувати до потреб конкретного бізнесу.

– Гнучкість. Можливість налаштування та кастомізації під індивідуальні вимоги.

– Доступність. Низька вартість володіння та експлуатації.

– Масштабованість. Рішення легко масштабуються для задоволення потреб, що зростають.

– Простота. Легкість впровадження, використання та адміністрування.

– Підтримка. Високий рівень зовнішньої сервісної підтримки.

Існують певні відмінності SMB-сегменту від корпоративного та державного сегментів:

– Стандартизація. На відміну від персоналізованих рішень для великих компаній, SMB-сегмент пропонує стандартизовані, оптимізовані та економічні рішення.

– Економічність. SMB-рішення розроблені з акцентом на доступність та економічну вигоду.

Пандемія COVID-19 мала значний вплив на кібербезпеку. Це спричинило такі наслідки, як зростання віддаленої роботи (пандемія призвела до масового переходу на віддалену роботу, що розширило доступ до корпоративних даних та

інформації), збільшення кібератак (цей фактор спричинив значне зростання кількості та складності кіберзлочинів, включаючи атаки з використанням програм-вимагачів), фінансові збитки (кібератаки можуть призвести до значних фінансових втрат для бізнесу, включаючи втрату даних, простої, викуп за розблокування даних та інші збитки).

Статистика кіберзлочинів, які відбуваються щодня в усьому світі, показує невтішні цифри, які вказують на такі показники, як:

– Глобальні втрати: у 2022 році глобальні втрати від кібератак становили 4,4 мільйона доларів.

– Середня вартість витоку даних: 4,35 мільйона доларів.

– Найдорожча галузь: охорона здоров’я (10,1 млн доларів).

– Економія від попередження витоку: 1,12 млн доларів протягом 200 днів або менше.

– Вартість атаки програм-вимагачів: 4,54 млн доларів.

– Вартість атаки на інфраструктуру: 5,12 млн доларів.

– Важливість плану реагування: організації, які перевірили свій план реагування на інциденти, заощадили 2,66 млн доларів порівняно з тими, хто цього не зробив.

Сьогодні питання кібербезпеки стає все більш критичним для бізнесу в усіх сегментах, особливо в SMB-сегменті. Використання доступних та надійних рішень кібербезпеки, а також впровадження ефективних стратегій захисту даних є життєво важливими для мінімізації ризиків та збитків від кіберзлочинів.

Середня вартість витоку даних від кібератак у розрізі галузей представлена на рисунку 1.1.

Рисунок 1.1 – Середня вартість витоку даних від кібератак у розрізі галузей

На сьогодні жодна компанія, незалежно від її розміру, не може ігнорувати кіберзагрози. Зловмисники стають винахідливішими, атаки частішають, а шкода від них зростає. Це відбувається через зростання кіберзлочинності, оскільки злочинці постійно шукають нові шляхи проникнення в корпоративні мережі, крадіжки цінних даних та завдання шкоди. Також причиною є поширення віддаленої роботи: перехід на віддалену роботу розширив поле для атак, створивши нові вразливі місця. Недостатня увага до кібербезпеки теж є причиною, оскільки багато компаній, особливо малих та середніх, нехтують питаннями кібербезпеки через брак бюджету або помилкове відчуття захищеності.

Серед наслідків кібернебезпеки є наступні:

– Фінансові втрати. Витік даних може коштувати компаніям мільйони доларів через втрату клієнтів, штрафи за невідповідність нормам, простої та інші збитки.

– Пошкодження репутації. Втрата довіри клієнтів може мати руйнівний вплив на репутацію та майбутнє компанії.

– Зниження продуктивності. Кібератаки можуть призвести до простоїв систем, що негативно впливає на роботу всієї компанії.

Інвестуючи в кібербезпеку та впроваджуючи надійні системи захисту та постійне навчання персоналу, можна впливати на ключові фактори для запобігання кібератакам. Важливо також використовувати сучасні технології: штучний інтелект та автоматизація можуть значно посилити кібербезпеку та допомогти швидше реагувати на загрози. Значним захистом слугує також підвищення обізнаності: важливо, щоб усі співробітники розуміли ризики кіберзлочинності та знали, як діяти у разі атаки.

Кібербезпека - це не витрата, а інвестиція в майбутнє вашого бізнесу. За останніми статистичними даними,

- 54% керівників IT-відділів зазнали кібератаки протягом останнього року.
- 6,7% доходу в середньому втрачають компанії через кібератаки.
- Малі та середні підприємства складають майже половину жертв кібератак.
- Лише 14% малих та середніх підприємств впровадили заходи з кібербезпеки.
- Витік даних може коштувати малому бізнесу в середньому 2,98 млн доларів США.

Малий та середній бізнес (SMB) – це не лише основа світової економіки, але й головне джерело робочих місць (95% підприємств та 60-70% працівників). Їх розвиток є ключовим фактором стабільності будь-якої країни. SMB, від сімейних ресторанів до стартапів, становлять 90% компаній у світі та генерують понад 50% робочих місць. Їхня вразливість до кіберзлочинів робить їх мішенню для атак, що може призвести до простою, фінансових втрат або навіть закриття. Захист кібербезпеки SMB – це не лише економічне, але й питання безпеки.

Пандемія COVID-19 змусила SMB швидко освоїти нові цифрові стратегії та технології, часто в умовах дистанційної роботи.

Це призвело до зростання кіберризиків: атаки відбуваються що 39 секунд (2244 рази на добу), а вразливість SMB до кіберзлочинів щорічно зростає на 400%.

Питання вартості кібератак формує на сьогодні попри все, хибне уявлення про те, що SMB менш вразливі до кібератак, є небезпечним. Дослідження у Великій Британії показало, що середня вартість успішної кібератаки на SMB становить 3230 фунтів стерлінгів. Це може призвести до закриття 25% SMB та скорочення штату на 16%. Втрата репутації та довіри клієнтів може мати ще довгостроковіші наслідки. 81% споживачів відмовляться від бренду після витоку даних.

Ланцюг постачання:

- SMB співпрацюють з численними постачальниками та партнерами, і їхні дані так само цінні, як і дані великих компаній.
- Злом однієї ланки ланцюга постачання може полегшити атаку на інші, часто більші, ланки.
- Дані SMB зазвичай легше вкрасти, що робить їх ласою здобиччю для хакерів.
- Кібератаки на SMB стають все більш частими, складними та організованими.

Отже, захист кібербезпеки – це критичне питання для SMB, яке не можна ігнорувати.

Інвестування в кіберзахист може допомогти SMB уникнути значних фінансових втрат, шкоди репутації та простоїв.

Доступні різні рішення кібербезпеки, які відповідають потребам та бюджету SMB.

Важливо, щоб SMB знали про ризики кібербезпеки та вживали заходів для їх мінімізації.

Існують безкоштовні та платні ресурси, які можуть допомогти SMB у захисті їх даних та систем. Уряд та приватний сектор можуть співпрацювати, щоб допомогти SMB підвищити рівень кібербезпеки.

Зростання кіберзагроз для SMB передусім означає:

- Злам програмного забезпечення, а не пристроїв. При цьому зловмисники все частіше використовують шкідливий код, вбудований в оновлення програмного забезпечення, для атак на SMB.

- Вразливість ланцюгів постачання. Атаки на SMB часто здійснюються через їх ланцюги постачання, де хакери можуть отримати доступ до конфіденційних даних.
- Використання SMB як трампліну. Зловмисники використовують атаки на SMB як плацдарм для проникнення в більші організації.
- Бібліотеки з відкритим кодом. Бібліотеки з відкритим кодом в ланцюгах постачання також можуть бути джерелом вразливостей.
- Зростання IoT. Зростання кількості IoT-пристроїв до 75 мільярдів до 2025 року створює нові ризики, адже багато з них будуть вразливими до кібератак.
- IT/OT-технології та ланцюги постачання. Розширення екосистеми IT/OT-технологій та ланцюгів постачання робить SMB більш вразливими до комплексных атак.

Часто SMB ігнорують кібербезпеку через відсутність дій: 93% власників SMB вважають кібербезпеку критичною, але лише 64% використовують засоби захисту. Деякі SMB помилково вважають, що кібербезпекові інструменти вже вбудовані в IT-продукти, які вони купують. Ігнорують кібербезпеку також через небажання інвестувати: середній рівень інвестицій в кібербезпеку для SMB становить 5100 фунтів стерлінгів, що може здатися їм незначним. Значну роль в цьому також відіграє неспроможність конкурувати з великими компаніями: великі організації інвестують значно більше в кібербезпеку (277 тисяч фунтів стерлінгів), що дає їм значну перевагу.

Значною мірою сьогодні зростає вартість кібератак: середня вартість успішної кібератаки на SMB становить 3230 фунтів стерлінгів, що може призвести до закриття 25% SMB та скорочення штату на 16%, втрати репутації: 81% споживачів відмовляться від бренду після витоку даних. Також стає актуальним питанням питання доступності рішень: існують різноманітні рішення кібербезпеки, які відповідають потребам та бюджету SMB. Важливою є обізнаність: SMB повинні знати про ризики кібербезпеки та вживати заходів для їх мінімізації. Актуальним питанням стає не лише фінансування зарубіжними джерелами тих або інших проєктів, спрямованих на захист програмного забезпечення підприємств, а й

допомога від уряду та приватного сектору: Уряд та приватний сектор можуть співпрацювати, щоб допомогти SMB підвищити рівень кібербезпеки.

Отже, кібербезпека стає все більш критичною для SMB, адже ризики зростають. SMB повинні вживати заходів для захисту своїх даних та систем, щоб уникнути значних фінансових втрат, шкоди репутації та простоїв. Доступні різні ресурси, які можуть допомогти SMB у цьому.

Фактори, що роблять SMB вразливими:

- Нерозвинена «кіберкультура»: досить багато SMB, працюючи роками, досі не мають чіткої стратегії кібербезпеки та не навчають своїх співробітників основам захисту даних.
- Страх перед хмарами: деякі SMB помилково вважають, що хмарні технології складні та небезпечні, тому не використовують їхні переваги для підвищення кібербезпеки.
- Хибні уявлення та нестача знань: SMB часто не знають про доступні їм технології та ресурси для захисту від кіберзагроз.
- Недостатнє навчання співробітників: 54% SMB не проводять навчання з питань кібербезпеки для своїх співробітників, що робить їх вразливими до фішингу та інших соціальних інженерних атак.

SMB стають мішенню, через слабкий захист, оскільки вони часто мають менш стійкі системи кібербезпеки, що робить їх легшою мішенню для хакерів. Через шлях до більших цілей зловмисники можуть використовувати SMB як трамплін для проникнення в більші та цінніші організації. Через використання відомих вразливостей хакери часто використовують давно відомі вразливості, для яких вже існують патчі, що свідчить про недбале ставлення SMB до оновлення своїх систем. Через необережність користувачів SMB можуть постраждати, через недбалість своїх співробітників, які відкривають листи та вкладення від невідомих відправників.

Неможливість запобігти атакам, але можливість захисту:

- Антивіруси та фаєрволи не дають 100% гарантії: Ці інструменти можуть зупинити автоматизовані атаки, але не зупинять кваліфікованих хакерів.

– Моніторинг інфраструктури: Постійний моніторинг мереж та систем SMB в режимі реального часу може допомогти виявити атаки на ранніх стадіях.

– Швидке реагування: SMB повинні мати чіткий план дій на випадок кібератаки, щоб мінімізувати шкоду.

Кібербезпека є пріоритетною незалежно від розміру, SMB повинні ставити кібербезпеку на перше місце. Захист даних та систем від атак є критичним фактором для успіху SMB. Ефективна кібербезпека потребує комплексного підходу, що включає людей, процеси, системи, мережі та технології. Єдине бачення, культура та цінності SMB щодо кібербезпеки є ключовими для успішного захисту.

Підвищення обізнаності – це ключ до захисту, оскільки SMB повинні знати про сучасні кіберзагрози та максимально розуміти їхні ризики. Є важливими навчання та освіта співробітників з питань кібербезпеки. Чим вищою є обізнаність SMB про кіберзагрози, тим краще вони зможуть захистити себе.

Отже, SMB не повинні ігнорувати кібербезпеку. Інвестування в захист даних та систем може допомогти їм уникнути значних фінансових втрат, шкоди репутації та простоїв. Доступні різні ресурси, які можуть допомогти SMB у цьому.

1.2 Основні компоненти IT інфраструктури та типові кіберзагрози

IT-інфраструктура є досить важливою, оскільки - це основа будь-якого сучасного бізнесу. Це є комплексна система, що об’єднує всі комп’ютери, мережі, програмне забезпечення та інші ресурси, які використовує підприємство для ведення своєї діяльності. Ефективна IT-інфраструктура допомагає:

– Уникати збоїв у роботі: Збої в IT-системі можуть призвести до значних фінансових втрат та шкоди репутації. Надійна IT-інфраструктура допомагає мінімізувати ризики та забезпечити безперебійну роботу бізнесу.

– Ефективно управляти активами: IT-інфраструктура дає можливість чітко бачити та контролювати всі IT-активи підприємства, від комп’ютерів до

програмного забезпечення. Це допомагає оптимізувати витрати, планувати оновлення та забезпечувати безпеку даних.

- Масштабувати бізнес: Коли бізнес росте, його IT-інфраструктура повинна рости разом з ним. Надійна та гнучка IT-інфраструктура дозволяє легко додавати нових користувачів, відкривати нові офіси та впроваджувати нові технології.
- Захищати дані: Дані - це один з найцінніших активів будь-якого підприємства. IT-інфраструктура повинна забезпечувати надійний захист даних від кіберзагроз, витоків та втрат.
- Знижувати витрати: Ефективна IT-інфраструктура може допомогти підприємству значно знизити витрати на IT, завдяки автоматизації рутинних завдань, оптимізації використання ресурсів та кращому плануванню закупівель.

З чого складається IT-інфраструктура?

IT-інфраструктура підприємства умовно складається з трьох основних компонентів:

- Апаратне забезпечення: Це фізична частина IT-інфраструктури, яка включає сервери, комп'ютери, мережеві пристрої, системи зберігання даних та інше обладнання.
- Програмне забезпечення: Це програмні продукти, які забезпечують роботу апаратного забезпечення та надають користувачам необхідні функції. До програмного забезпечення належать операційні системи, прикладні програми, антивірусне програмне забезпечення та багато іншого.
- Мережа: Це система, яка з'єднує всі пристрої IT-інфраструктури та забезпечує їм можливість обмінюватися даними. Мережа може бути локальною (в межах одного офісу або будівлі) або глобальною (з'єднує офіси в різних містах або країнах).

Організація IT-інфраструктури залежить від потреб та цілей конкретного підприємства. Однак деякі принципи є універсальними:

- Відповідність бізнес-задачам: IT-інфраструктура повинна відповідати потребам бізнесу та допомагати йому досягати своїх цілей.

- Надійність та безпека: IT-інфраструктура повинна бути надійною та безпечною, щоб забезпечити безперебійну роботу бізнесу та захистити його дані.
- Масштабованість: IT-інфраструктура повинна бути легко масштабованою, щоб вона могла рости разом з бізнесом.
- Ефективність: IT-інфраструктура повинна бути ефективною та економною, щоб вона не обтяжувала бюджет підприємства.

Для забезпечення безперебійної роботи IT-інфраструктури потрібна кваліфікована підтримка. Це може бути власна IT-служба підприємства або сторонній постачальник послуг.

Програмне забезпечення IT-інфраструктури – це програмне забезпечення, яке використовується для роботи з апаратною частиною та її управління. До нього належать:

- Операційні системи
- Драйвери
- Утиліти
- Бібліотеки
- Бази даних
- Системи управління сайтом (CMS)
- Системи управління взаємовідносинами з клієнтами (CRM)
- Поштові клієнти
- Інші послуги

Мережева інфраструктура необхідна для забезпечення роботи внутрішньої та зовнішньої мережі. До неї належать:

- Маршрутизатори
- Комутатори
- Брандмауери
- Серверне обладнання
- Мережеве програмне забезпечення

Мережа може складатися з програмних і апаратних компонентів. Взаємодія компонентів IT-інфраструктури є наступною. Ці три складові - апаратне

забезпечення, програмне забезпечення та мережа - взаємодіють між собою, щоб створити функціональну та ефективну IT-інфраструктуру. IT-інфраструктура підтримує діяльність підприємства та забезпечує його потреби у зв'язку, обробці та збереженні даних.

Важливість IT-інфраструктури полягає у тому, що ефективна IT-інфраструктура забезпечує:

- Ефективну роботу компанії
- Конкурентоспроможність товарів та послуг на ринку
- Оптимізацію витрат підприємства
- Підвищення продуктивності IT-сервісів

В даний час це актуально практично у всіх галузях, адже комп'ютерні технології та інтернет проникли всюди.

Моделі IT-інфраструктури:

вибір типу та моделі IT-інфраструктури залежить від потреб компанії, її бюджету, гнучкості та безпеки.

Існує кілька варіантів:

1. Традиційна модель:
   - Компанія закуповує власне обладнання
   - Розміщує його всередині офісу або у провайдера
2. Хмарна модель:
   - Компоненти інфраструктури розміщені у хмарного провайдера
   - Хмарний провайдер надає технічне забезпечення та керування віддалено
3. Комбінована модель:
   - Частина інфраструктури розміщується на боці компанії
   - Частина - у хмарі

Важливо ретельно розглянути всі аспекти перед прийняттям рішення про тип IT-інфраструктури. Схема комбінованої моделі IT інфраструктури представлена на рисунку 1.2.

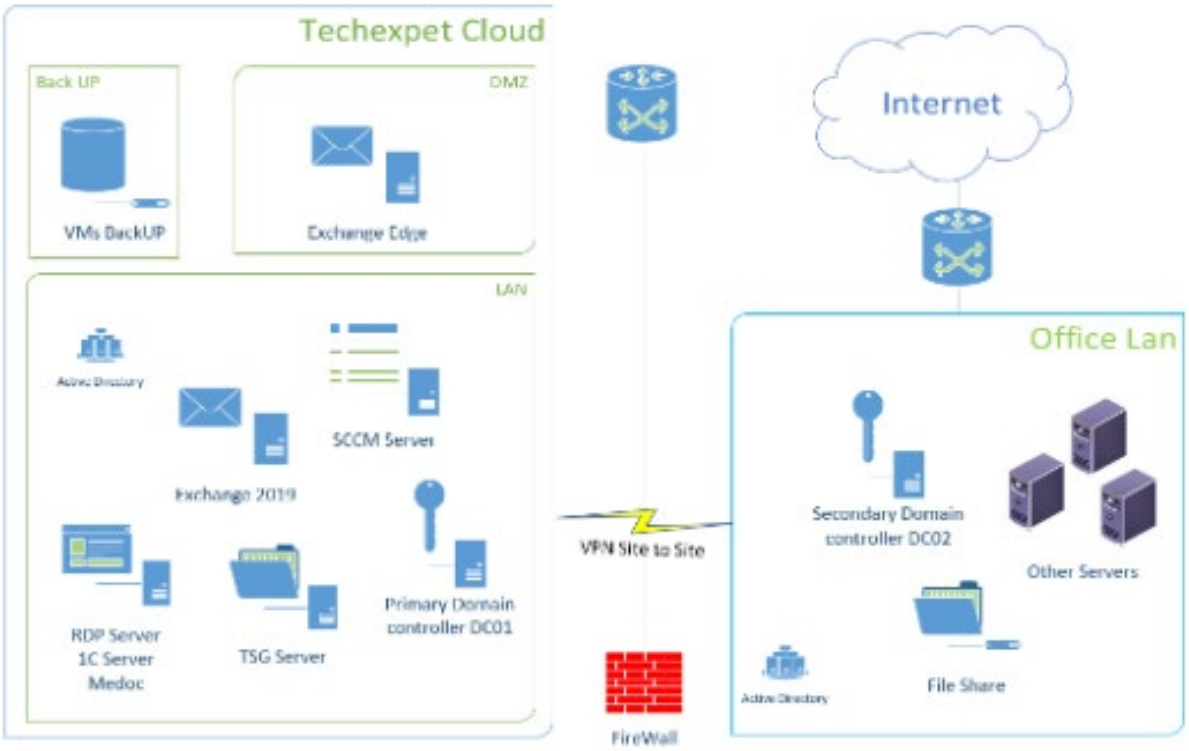


Рисунок 1.2 – Схема комбінованої моделі IT інфраструктури

Хмарна IT-інфраструктура: зручне рішення для малого та середнього бізнесу

Хмарна IT-інфраструктура стає все більш популярним вибором для малого та середнього бізнесу. Вона пропонує ряд переваг, таких як:

1. Зниження витрат. Не потрібно купувати та обслуговувати дороге обладнання.
2. Гнучкість. Легко масштабувати інфраструктуру вгору або вниз у міру зростання або зменшення потреб.
3. Доступність. Доступ до інфраструктури з будь-якого місця з підключенням до Інтернету.
4. Надійність. Хмарні провайдери пропонують високий рівень надійності та доступності.
5. Безпека. Хмарні провайдери мають суворі заходи безпеки для захисту ваших даних.

Основні компоненти хмарної IT-інфраструктури:

- Мережева інфраструктура. Забезпечує підключення до Інтернету та зв’язок між різними компонентами інфраструктури.
- Серверна інфраструктура. Включає віртуальні сервери, які хостять ваші веб-сайти, програми та дані.
- Робочі станції. Користувачі можуть отримувати доступ до своїх робочих станцій з будь-якого пристрою з підключенням до Інтернету.
- Електронна пошта. Хмарні служби електронної пошти пропонують надійне та зручне рішення для спілкування.
- Система моніторингу. Дозволяє відстежувати продуктивність та безпеку вашої інфраструктури.
- Система резервного копіювання. Забезпечує захист ваших даних від втрати.

Переваги хмарної IT-інфраструктури для малого та середнього бізнесу:

- Зниження витрат. Не потрібно купувати та обслуговувати дороге обладнання.
- Збільшена продуктивність. Хмарні служби можуть допомогти вам підвищити продуктивність співробітників.
- Підвищена конкурентоспроможність. Хмарні технології можуть дати вам конкурентну перевагу.
- Зменшення IT-витрат. Хмарні служби можуть допомогти вам заощадити на IT-витратах.
- Покращена безпека. Хмарні провайдери пропонують високий рівень безпеки для захисту ваших даних.

Отже, хмарна IT-інфраструктура може бути вигідним рішенням для малого та середнього бізнесу, бо вона пропонує ряд переваг.

Схема основних компонентів та сервісів IT інфраструктури представлена на рисунку 1.3.

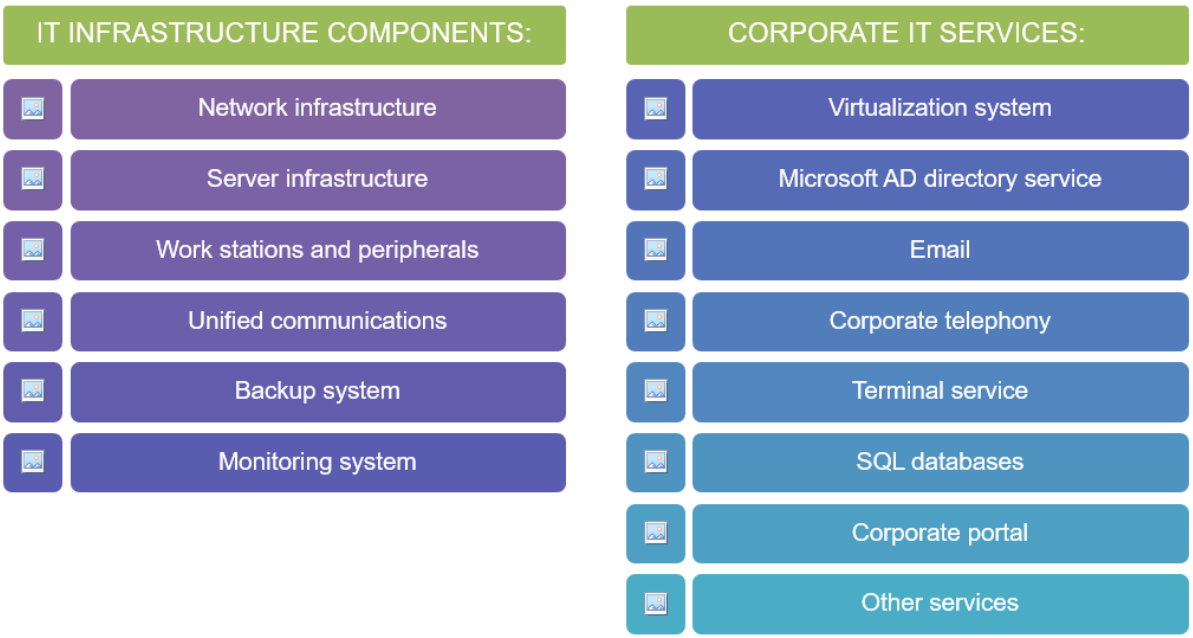


Рисунок 1.3 – Схема основних компонентів та сервісів IT інфраструктури

Кіберзагрози – це події або обставини, які можуть негативно вплинути на діяльність SMB, завдаючи шкоди їхнім функціям, репутації, активам або персоналу. Ці загрози можуть проявлятися у вигляді несанкціонованого доступу до інформаційних систем, знищення або модифікації конфіденційних даних.

Які основні методи кіберзловмисників, які полюють на SMB?

– Фішинг та соціальна інженерія: Хакери використовують ці методи, щоб обманом змусити співробітників SMB розкрити конфіденційну інформацію, таку як паролі, номери кредитних карток або інші дані. Це може відбуватися через електронні листи, телефонні дзвінки, соціальні мережі або інші канали.

– Експлуатація вразливостей в ланцюгу постачання: Хакери можуть атакувати SMB через їхніх постачальників або партнерів, які мають доступ до їхніх систем або даних.

– Певні фактори роблять SMB більш вразливими до кіберзагроз. Це такі фактори, як:

– Недостатня оцінка ризиків: SMB часто не мають ресурсів або знань для належної оцінки своїх кіберризиків.

– Недостатній контроль доступу: SMB можуть не мати чітких правил доступу до своїх систем та даних, що робить їх більш вразливими до несанкціонованого доступу.

– Недостатній захист даних: SMB можуть не мати належних заходів для захисту своїх даних від крадіжки або пошкодження.

– Слабкі паролі: SMB можуть використовувати слабкі або легко вгадувані паролі для своїх систем та даних.

– Недостатня обізнаність та навчання: Співробітники SMB можуть не знати про кіберзагрози або про те, як їм протистояти.

– Відсутність культури кібергігієни: SMB можуть не мати чітких правил та процедур для захисту своїх систем та даних від кіберзагроз.

Які найпоширеніші кіберзагрози, з якими стикаються SMB?

– Фішинг: Як описано вище, фішинг – це метод, який використовують хакери, щоб обманом змусити людей розкрити конфіденційну інформацію.

– Шкідливе програмне забезпечення: шкідливе програмне забезпечення, таке як віруси, хробаки та трояни, може завдати значної шкоди SMB, включаючи втрату даних, фінансові втрати та шкоду репутації.

– Програми-здирники: програми-здирники шифрують дані SMB і вимагають викуп за їх розшифрування. Ці атаки можуть бути руйнівними для SMB, спричиняючи значні фінансові збитки та перебої в роботі.

– DDoS-атаки: DDoS-атаки перевантажують веб-сайти або мережі SMB трафіком, що призводить до їх виходу з ладу. Ці атаки можуть спричинити значні перебої в роботі та фінансові втрати.

– Інсайдерські загрози: інсайдерські загрози виникають, коли співробітники або підрядники SMB навмисно або ненавмисно ставлять під загрозу безпеку компанії.

– Атаки на паролі: хакери можуть використовувати різні методи, щоб отримати доступ до систем SMB, вгадуючи або зламуючи паролі.

– Соціальна інженерія - метод, який використовують хакери, щоб обманом змусити людей розкрити конфіденційну інформацію.

– SMB можуть захистити себе від кіберзагроз багатьма способами та засобами, головне при цьому розуміти всю ступінь відповідальності. Існує багато кроків, які SMB можуть зробити, щоб захистити себе від кіберзагроз:

– Провести оцінку ризиків: SMB повинні регулярно оцінювати свої кіберризики, щоб визначити, яким загрозам вони піддаються.

– Впровадити контроль доступу: SMB повинні мати чіткі правила доступу до своїх систем та даних, щоб обмежити доступ лише авторизованим користувачам.

– Захистити дані: SMB повинні використовувати належні заходи для захисту своїх даних від крадіжки або пошкодження. Це може включати шифрування даних, резервне копіювання даних та використання брандмауерів та антивірусного програмного забезпечення.

– Використовувати сильні паролі: SMB повинні вимагати від своїх співробітників використовувати сильні та унікальні паролі для своїх систем та даних.

– Навчити співробітників: SMB повинні навчати своїх співробітників про кіберзагрози та про те, як їм протистояти. Це може включати навчання з питань фішингу, соціальної інженерії та безпеки паролів.

– Впровадити культуру кібергігієни: SMB повинні мати чіткі правила та процедури для захисту своїх систем та даних від кіберзагроз. Це може включати регулярне оновлення програмного забезпечення, використання надійних паролів та уникання відкриття підозрілих посилань або вкладення файлів.

– Використовувати послуги кібербезпеки: SMB можуть скористатися послугами кібербезпеки, щоб допомогти їм захистити свої системи та дані. Ці послуги можуть включати тестування на проникнення, моніторинг мережі та реагування на інциденти.

Кіберзагрози – це надсерйозна проблема для SMB. Однак, вживаючи превентивних заходів, SMB можуть значно знизити ризик кібератаки. Важливо,

щоб SMB розуміли кіберзагрози, з якими вони стикаються, та вживали заходів для захисту себе.

Фішинг та соціальна інженерія: маніпуляції в епоху цифрових технологій. Із 85% кібератак починаються з фішингових атак, які стають все більш досконалими завдяки штучному інтелекту.

– Соціальна інженерія використовує психологічні методи, щоб змусити людей розкрити конфіденційну інформацію.

– Пандемія COVID-19 стала сприятливим середовищем для кібершахраїв, які використовують фішинг та соціальну інженерію для крадіжки особистих даних.

Еволюція кіберзагроз: від Morris Worm до сучасних програм-вимагачів

– Рівень розвитку кіберзагроз значно зріс з часів першої кібератаки Morris Worm у 1988 році.

– Програми-вимагачі стають все більш поширеними, завдаючи SMB значної шкоди.

– Дослідження показують, що кожне п’яте SMB стає жертвою програм-вимагачів, а середній розмір викупу становить 6 000 доларів.

– Витрати на відновлення після атаки програми-вимагача можуть сягати 141 000 доларів, не рахуючи шкоди репутації та втрачених даних.

SMB часто не мають достатніх ресурсів для захисту від кіберзагроз. У деяких з них - нестача персоналу, обмежений бюджет та відсутність обізнаності роблять SMB вразливими. Співробітники SMB можуть не розпізнавати потенційні кіберзагрози, що робить їх мішенями для атак.

Недооцінювання важливості навчання з питань кібербезпеки може завдати шкоди SMB в довгостроковій перспективі.

Захист від програм-вимагачів має результативний комплексний підхід, який полягає в тому, що враховуються всі можливі загрози і в процесі діяльності та використання ПЗ ігноруються потенційно небезпечні фактори загроз: наприклад: оплата викупу не гарантує відновлення даних та фінансує кіберзлочинність. SMB повинні вживати заходів для запобігання атакам програм-вимагачів.

До базових рекомендацій та комплексу дій з кібербезпеки належать: використання надійних паролів та багатофакторної автентифікації; регулярне оновлення програмного забезпечення та операційної системи; створення резервних копій даних; навчання співробітників основам кібербезпеки; використання надійних антивірусних програм та брандмауерів. розробка плану реагування на кіберінциденти.

Кіберзагрози – це на сьогодні дуже серйозна проблема для SMB. Вживаючи заходів для запобігання атакам та навчаючи персонал основам кібербезпеки, SMB можуть мінімізувати або взагалі виключити можливість виникнення загроз та роботу над їх усуненням.

1.3 Висновки до першого розділу

В результаті дослідження та аналізу питань у першому розділу роботи встановлено, що в нинішній час захист малого та середнього бізнесу від кіберзагроз має дуже важливе значення в сучасну цифровому світі. Загрози на основні компоненти IT інфраструктури малих та середніх підприємств постійно зростають, змінюються, маневрують та завдають непоправної шкоди. Розуміючи найпоширеніші загрози кібербезпеки, компанії SMB сегменту можуть запобігати кібератакам, мінімізувати їх наслідки та зберегти свій бізнес у безпеці. Для цього необхідно завжди бути в курсі останніх кіберзагроз та найкращих практик, впроваджувати ефективні методи та засоби підвищення рівня кіберзахисту захисту, опановувати інструменти та проводити комплекс дій по виявленню та аналізу вразливостей основних компонентів IT інфраструктури, а також не соромитись звертатися за допомогою до професіоналів з кібербезпеки, якщо це необхідно.

РОЗДІЛ 2
МЕТОДИ ТА ЗАСОБИ ПІДВИЩЕННЯ РІВНЯ КІБЕРЗАХИСТУ ІТ ІНФРАСТРУКТУРИ

2.1 Організаційні заходи заберзпечення кібербезпеки на підприємстві

Організаційні заходи забезпечення кібербезпеки – це цілий комплекс заходів, спрямованих на захист інформаційних систем та даних підприємства від несанкціонованого доступу, використання, розголошення, порушення цілісності або знищення.

До основних організаційних заходів забезпечення кібербезпеки належать:

– Розробка та впровадження політики кібербезпеки. Політика кібербезпеки повинна чітко визначати відповідальність за кібербезпеку на підприємстві, встановлювати правила поведінки для співробітників та описувати процедури реагування на кіберінциденти.

– Підготовка та навчання персоналу. Співробітники – це перша лінія оборони від кібератак. Тому важливо проводити регулярні навчання персоналу з питань кібербезпеки, щоб навчити їх розпізнавати та уникати кіберзагроз.

– Захист інформаційних систем. Інформаційні системи підприємства повинні бути захищені за допомогою брандмауерів, антивірусного програмного забезпечення та інших систем безпеки.

– Управління вразливостями. Підприємства повинні регулярно сканувати свої інформаційні системи на наявність вразливостей та вживати заходів щодо їх усунення.

– Резервне копіювання та відновлення даних. Важливо регулярно створювати резервні копії даних підприємства, щоб мати можливість відновити їх у разі кібератаки.

– Контроль доступу. Підприємства повинні впровадити систему контролю доступу, яка дозволить надавати доступ до інформаційних систем лише уповноваженим користувачам.

– Управління інцидентами. Підприємства повинні мати план реагування на кіберінциденти, який дозволить їм швидко та ефективно реагувати на кібератаки.

Деякі зарубіжні американські джерела, які вивчають організаційні заходи забезпечення кібербезпеки, публікують ряд публікацій з питань кібербезпеки, включаючи NIST Cybersecurity Framework (Національний інститут стандартів і технологій (NIST): NIST), Агентство з кібербезпеки та інфраструктурної безпеки (CISA): CISA надає ресурси та послуги для допомоги підприємствам у захисті своїх мереж від кібератак. Федеральна торгова комісія (FTC): FTC надає інформацію про те, як підприємства можуть захистити своїх клієнтів від кібершахрайства. Асоціація комп'ютерної індустрії (CIA): CIA публікує дослідження та звіти з питань кібербезпеки.

В епоху цифрових технологій кіберзагрози стають все більш небезпечними. SMB, які не вживають заходів для захисту своїх даних, ризикують стати жертвами кібератак, що може призвести до значних фінансових втрат, шкоди репутації та навіть банкрутства.

Не існує універсального підходу до кібербезпеки, оскільки кожен бізнес має свої унікальні ризики. Однак SMB можуть вжити ряд заходів для захисту своїх даних, таких як:

Оцінка ризиків: SMB повинні визначити свої унікальні ризики кібербезпеки та розробити план їх пом'якшення.

Моделювання загроз: цей процес допомагає SMB краще зрозуміти potential threats and develop strategies to protect themselves.

Аналіз загроз: цей процес допомагає SMB виявити вразливості в своїх системах безпеки.

Впровадження заходів безпеки: SMB повинні використовувати різні заходи безпеки, такі як брандмауери, антивірусне програмне забезпечення та шифрування даних.

Навчання персоналу: співробітники SMB повинні знати про кіберзагрози та знати, як їх розпізнавати та уникати.

Моделювання загроз – це метод оцінки потенційних кіберзагроз, яким може піддаватися SMB. Цей процес включає в себе:

1. Визначення активів: SMB повинне визначити всі свої активи, які потребують захисту, такі як дані, системи та програмне забезпечення.

2. Ідентифікацію загроз: SMB повинне ідентифікувати всі потенційні кіберзагрози, які можуть вплинути на його активи. Це може включати в себе хакери, шкідливе програмне забезпечення, фішингові атаки та інші.

3. Оцінку ризиків: SMB повинне оцінити ймовірність та потенційний вплив кожної загрози.

4. Розробку заходів безпеки: SMB повинне розробити та впровадити заходи безпеки для пом'якшення ризиків, пов'язаних з кожною загрозою.

Існує декілька методів моделювання загроз, які можуть використовувати SMB. Найпоширеніші методи включають:

– Аналіз активів: Цей метод включає в себе інвентаризацію всіх активів SMB та оцінку їх цінності та вразливості.

– Аналіз загроз: Цей метод включає в себе дослідження та ідентифікацію потенційних кіберзагроз, які можуть вплинути на SMB.

– Аналіз вразливостей: Цей метод включає в себе сканування систем та програмного забезпечення SMB на наявність вразливостей, які можуть бути використані кіберзлочинцями.

– Оцінка ризиків: Цей метод включає в себе оцінку ймовірності та потенційного впливу кожної загрози.

– Розробка заходів безпеки: Цей метод включає в себе розробку та впровадження заходів безпеки для пом'якшення ризиків, пов'язаних з кожною загрозою.

– Моделювання загроз має велике значення для SMB, адже воно може допомогти їм:

– Підвищити рівень кібербезпеки: Моделювання загроз може допомогти SMB виявити та усунути вразливості до того, як ними скористаються кіберзлочинці.

– Знизити ризики: Моделювання загроз може допомогти SMB знизити ризики фінансових втрат, шкоди репутації та інших негативних наслідків кібератаки.

– Оптимізувати витрати на кібербезпеку: Моделювання загроз може допомогти SMB зосередити свої ресурси на найбільш важливих заходах безпеки.

– Підвищити обізнаність: Моделювання загроз може допомогти підвищити обізнаність співробітників про кіберзагрози та навчити їх протистояти їм.

Отже, моделювання загроз - це важливий інструмент, який може допомогти SMB захистити свої активи та інтереси від кіберзагроз. Впровадження моделювання загроз може значно підвищити рівень кібербезпеки вашого бізнесу та знизити ризики кібератак. Моделювання загроз – це стратегічний процес, який допомагає SMB визначити вимоги безпеки компанії, виявити та кількісно оцінити загрози та вразливості та впровадити заходи з їх усунення.

Під час аналізу загроз працівники SMB можуть:

1. Поставити себе на місце зловмисників, щоб оцінити потенційний збиток.
2. Проаналізувати програмні мережі, бізнес-контекст та документацію користувачів на предмет вразливостей.
3. Виявити нестандартні способи компрометації даних.
4. Визначити недоліки в системах безпеки.

Переваги аналізу загроз:

- Підвищує обізнаність про зовнішні загрози.
- Заохочує нестандартне мислення.
- Допомагає виявити недоліки в системах безпеки.

Отже, кібербезпека - це невід’ємна частина ведення бізнесу в епоху цифрових технологій. SMB, які вживають заходів для захисту своїх даних, можуть значно знизити ризик кібератак і забезпечити свою стійкість.

Без моделювання загроз SMB не можуть знати, які ризики для них становлять кіберзагрози. Це може призвести до того, що вони не вживатимуть необхідних заходів для захисту своїх даних, що робить їх вразливими до кібератак.

Як проводиться моделювання загроз?

Моделювання загроз зазвичай складається з чотирьох етапів, які вказані на рисунку 2.1.

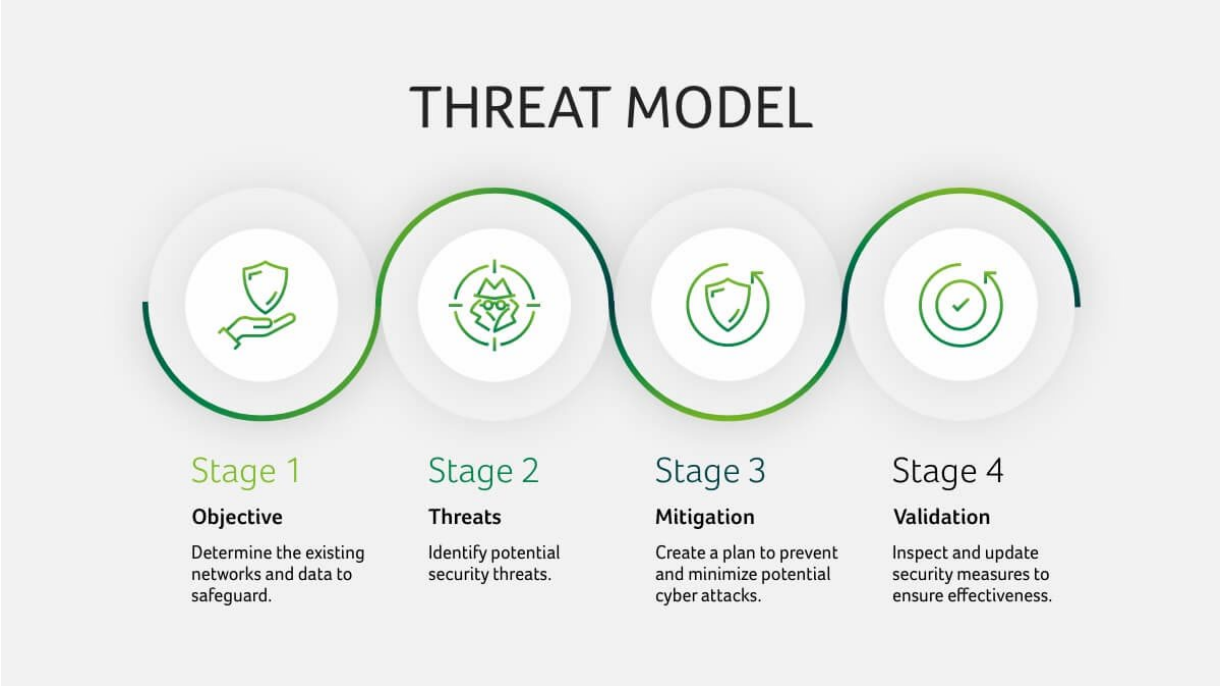


Рисунок 2.1 – Основні етапи моделі загроз

Етап 1: Постановка завдань: Цей етап включає визначення типу мережі, даних, які потрібно захистити, та бюджету на заходи безпеки.

Етап 2: Загрози: На цьому етапі фахівці з кібербезпеки визначають потенційні загрози, з якими може стикнутися SMB. Це може включати аналіз вразливостей мережі, типових загроз для галузі та методів, які використовують хакери.

Етап 3: Мінімізація ризиків: Після визначення загроз SMB розробляють план їх пом’якшення. Це може включати впровадження нових заходів безпеки, навчання персоналу та підвищення обізнаності про кібербезпеку.

Етап 4: Перевірка: На цьому етапі SMB регулярно перевіряють свою систему безпеки, щоб переконатися, що вона ефективна. Це може включати тестування на проникнення, аудит мережі та навчання з питань кібербезпеки.

Моделювання загроз може допомогти SMB захистити свої дані та системи від кібератак, зменшити ризики кібербезпеки, підвищити обізнаність про кібербезпеку, розробити ефективний план реагування на кіберінциденти.

Людський фактор у кібербезпеці має неабияке значення. Важливо пам’ятати, що люди – це найслабша ланка в ланцюзі кібербезпеки. Співробітники SMB можуть стати жертвами соціальної інженерії, фішингу та інших методів кібератак. Тому важливо навчати персонал основам кібербезпеки та вживати заходів для захисту їх від кіберзагроз.

Таким чином, моделювання загроз – це важливий інструмент, який може допомогти SMB захистити свої дані та системи від кібератак. Впровадження моделювання загроз може допомогти SMB значно знизити ризики кібербезпеки та забезпечити свою стійкість.

Кібергігієна – це не просто набір правил, а культура безпеки, яка визнає людей ключовим елементом захисту від кіберзагроз. Вона передбачає розуміння потенційних небезпек в Інтернеті, вміння їх визначати та уникати, а також знання про важливість технічних засобів захисту, таких як антивірусні програми та оновлення програмного забезпечення.

Співробітники SMB часто стають мішенню кіберзлочинців. Їхні помилки, такі як натискання на підозрілі посилання або розкриття конфіденційної інформації, можуть призвести до серйозних наслідків для SMB, таких як витік даних, фінансові втрати та шкода репутації.

SMB повинні регулярно проводити навчання для своїх співробітників з питань кібергігієни. Це допоможе їм зрозуміти базові принципи кібербезпеки, поширені загрози та методи захисту. Навчання з кібергігієни має зосереджуватися

на таких темах, як: кібербезпека та захист інформації: Співробітники повинні знати, як захищати свої персональні дані та конфіденційну інформацію в Інтернеті; основи кібергігієни: співробітники повинні навчитися ефективним стратегіям та технікам для уникнення кіберзагроз. Співробітники повинні знати про поширені шахрайські схеми, фішингові атаки та інші загрози, щоб їх розпізнавати та уникати. Співробітники повинні знати про принципи захисту інформації на робочому місці та в особистому житті. Співробітники повинні мати чіткі інструкції щодо безпечної роботи в Інтернеті та на робочому місці. SMB повинні регулярно проводити тренінги з кібербезпеки, щоб оновлювати знання своїх співробітників та знайомити їх з новими загрозами. SMB повинні надавати доступ до інформації та систем лише тим співробітникам, яким це дійсно необхідно. SMB повинні дозволяти встановлювати програмне забезпечення на пристрої компанії лише IT-персоналу.

Інформування співробітників про кіберзагрози та навчання їх основам кібергігієни – це важливий крок до захисту SMB від кібератак. Співробітники, які знають про ризики і знають, як їх уникнути, роблять SMB менш вразливими до кіберзлочинців.

Віддалений доступ до корпоративних мереж став невід'ємною частиною роботи для багатьох SMB. Однак це також відкриває нові можливості для кіберзлочинців. Хакери можуть використовувати вразливості в протоколах віддаленого доступу, таких як RDP, щоб отримати доступ до корпоративних мереж і завдати шкоди.

SMB можуть підвищити безпеку віддаленого доступу такими засобами та механізмами:

1. Використання надійних паролів та багатофакторної автентифікації: Співробітники повинні використовувати складні паролі для всіх корпоративних облікових записів. Багатофакторна автентифікація (MFA) додає додатковий рівень безпеки, вимагаючи від користувачів ввести другий фактор автентифікації, наприклад, код з одноразового пароля (OTP) або відбиток пальця.

2. Мінімізуючи ризики програм-вимагачів: відключивши або видаливши непотрібне програмне забезпечення та служби, щоб зменшити потенційні вектори атак для програм-вимагачів.

3. Обмеживши доступ до RDP: увімкнувши доступ до RDP з Інтернету або дозвольте його лише для певних авторизованих користувачів.

4. Впровадивши VPN: використовуючи VPN для створення безпечного зашифрованого тунелю між пристроєм користувача та корпоративною мережею.

5. Налаштувавши брандмауери: правильно налаштувавши брандмауери, щоб обмежити доступ до корпоративної мережі.

6. Оновлюючи програмне забезпечення: регулярно оновлюючи операційні системи та програмне забезпечення, щоб усунути відомі вразливості.

7. Навчаючи співробітників основам кібербезпеки та ознайомлюючи їх з ризиками віддаленого доступу.

Додаткові поради для безпечного віддаленого доступу:

– Використовувати антивірусне програмне забезпечення та системи EDR (Endpoint Detection and Response) для виявлення та запобігання кіберзагрозам.

– Застосовувати політику доступу з найменшими правами, щоб надати користувачам лише той доступ, який їм дійсно необхідний.

– Створити план реагування на інциденти на випадок кібератаки.

8. Використання системи брандмауера захищає корпоративну мережу від зовнішніх атак в першу чергу. З її допомогою ви можете відстежувати будь-який вхідний і вихідний трафік. Брандмауер може блокувати той чи іншій трафік, якщо він не відповідає політиці безпеки.

9. Необхідно впровадити служби моніторингу, реагування і виправлення різних збоїв для всіх користувачів, мереж і додатків. Щоб ці служби працювали без ускладнень, важливо підготувати їх до збільшення кількості пристроїв і процесів під час віддаленої роботи. Потрібно уважно ставитися до документації, яка містить конфіденційну інформацію. Справитися з цим завданням допоможе аудит корпоративних даних на всіх комп’ютерах [15].

10. Необхідно регулярно оновлювати операційні системи та інше програмне забезпечення, а також застосовувати всі виправлення відразу після виходу.

11. Важливо мати готовий план безперервної роботи бізнесу на випадок інцидентів. У ньому обов'язково має бути врахована наявність актуальної резервної копії всіх даних, а, можливо, навіть інфраструктури для резервного копіювання, яку ви можете використовувати під час спроби відновити роботу заблокованих систем.

12. Потрібно регулярно створювати резервні копії важливих для бізнесу даних і системно перевіряти коректність їх зберігання. Крім цього, найцінніші дані також повинні зберігатися в режимі офлайн.

Отже, захист віддаленого доступу – це важливе завдання для SMB. Впровадження описаних заходів безпеки може допомогти SMB захистити свої мережі від кіберзагроз і забезпечити безпеку своїх даних.

Під час налаштування брандмауерів для включення протоколу віддаленого робочого стола адміністратори мережі можуть або обмежити доступ до RDP лише для мережі компанії, або дозволити доступ через Інтернет. Однак відкриття портів для загального доступу становить небезпеку, адже таким чином хакери можуть їх виявити та атакувати [14].

Складний пароль – це добре, але багатофакторна автентифікація, в будь-якому випадку, не завадить. З її допомогою можна захистити пошту співробітників, корпоративні дані, ресурси, портали і хмарні додатки.

Потрібно системно шукати оптимальні варіанти захисту, звертатися до професіоналів для консультації. Адже будь-яка лазівка в системі захисту може коштувати не тільки грошей, але і витоку конфіденційних даних.

2.2 Інструменти та комплекс дій по виявленню та аналізу вразливостей основних компонентів IT інфраструктури

Компанія будь якого сегменту може зіштовхнутися з хакерською атакою, фішингом, диверсією, шкідливим програмним забезпеченням або іншими

кіберзагрозами. Для мінімізації вірогідності стати жертвою зловмисників та втратити корпоративні дані зконцентруємось на основних діях та інструментах по підвищенню кіберзахисту інфраструктури та IT сервісів малих та середніх компаній. Можна виділити кілька найбільш поширених причин, через які IT інфраструктура компаній SMB сегменту може бути недостатньо захищеною, а саме:

1. Слабка кібергігієна персоналу та відсутність управління доступом
2. Застарілі операційні системи та програмне забезпечення (ПЗ), яке не оновлюється.
3. Застарілі моделі серверного та мережевого обладнання.
4. Недостатньо захищена мережева інфраструктура.
5. Відсутність або неналежне використання систем моніторингу та резервного копіювання.

Наявність застарілих версій програмного забезпечення або операційних систем тягне за собою безліч критичних вразливостей та «слабких точок» в IT інфраструктурі, скористувавшись якими зовмисник може отримати контроль над IT сервісом та залишитись при цьому непоміченим. Використання застарілих версій ПЗ несе компаніям ризики злому IT інфраструктури з того моменту, як виробник припиняє випуск оновлень безпеки. Це означає, що всі виявлені та незакриті вразливості назавжди залишаються в продукті та можуть бути використані зловмисником. У більшості застарілого ПЗ відсутня підтримка сучасних методів шифрування даних при обміні інформацією між клієнтським та серверним ПЗ. Наприклад, Triple DES дозволяє перехватити та розшифрувати трафік або застаріла версія OpenSSL дозволяє проводити атаки Man-In-The-Middle [5,15].

Сучасне обладнання, на відміну від застарілого, підтримує більшу пропускну здатність, має спеціально вбудовані процесори для шифрування, підтримує нові протоколи та стандарти. Застарілі моделі не підтримують сучасні версії операційних систем, в результаті чого встановити необхідні актуальні оновлення, оновити сертифікати та патчі безпеки неможливо.

Захищена корпоративна мережа - це об’єднання територіально різних об’єктів (філіалів) в єдину інфраструктуру, централізований контроль та управління, розмежування доступу до мережі, логічний поділ мереж, постійний моніторинг провідних та бездротових мереж, мобільних пристроїв. На сьогодні більшість SMB компаній практикують частково віддалений режим роботи і тому стикаються зі слабозахищеними домашніми мережами, незахищеними віддаленими підключеннями, використанням публічних та хмарних сервісів - все це підвищує ризик перехвату трафіку, витоку даних тощо.

Відсутність хоча б базової системи моніторингу IT безпеки призведе до наступних проблем:

1. IT відділу буде складно підтримувати працездатність компонентів IT інфраструктури не маючи даних про навантаження на її елементи.
2. Зменшиться час реагування на вторнення в систему і, як наслідок, збільшиться час на відновлення працездатності після атак.
3. Розслідування інцидентів, пов’язаних з IT-безпекою компанії, стає практично неможливим, тому що відсутня чітка інформація, на підставі якої можна провести аналіз подій.

Моніторинг IT безпеки являє собою збір та аналіз інформації про роботу та навантаження на елементи інфраструктури, виявлення підозрілії активності та незрозумілих процесів. Якщо система моніторингу виявляє підозріле навантаження на ресурси, то створюються повідомлення та виконуються ряд дій щодо заходів безпеки. Скріншот системи моніторингу представлено на рисунку 2.2

Рисунок 2.2 – Скріншот системи моніторингу Zabbix

Система резервного копіювання даних є ключовим елементом в IT інфраструктурі та напряму впливає на доступність сервісів.

Дуже часто можна зустріти ситуації, коли в SMB-компаніях система створення та зберігання резервних копій або не налаштована, або відсутня зовсім (що є неприйнятним для сьогодення). Це означає, що внаслідок злому такої інфраструктури, втрати чи підміни будь-яких даних – швидко відновити систему чи окремі її файли, з мінімальним часом простою та забезпечення максимальної доступності бізнесу, буде проблематично чи навіть неможливо.

На рисунку 2.3 наведено приклад управління резервними копіями із системи Veeam. Ми бачимо назву завдання, загальну інформацію (розклад, статуси виконання, швидкість створення, час виконання тощо), список віртуальних чи фізичних хостів у завданні бекапу та результат.

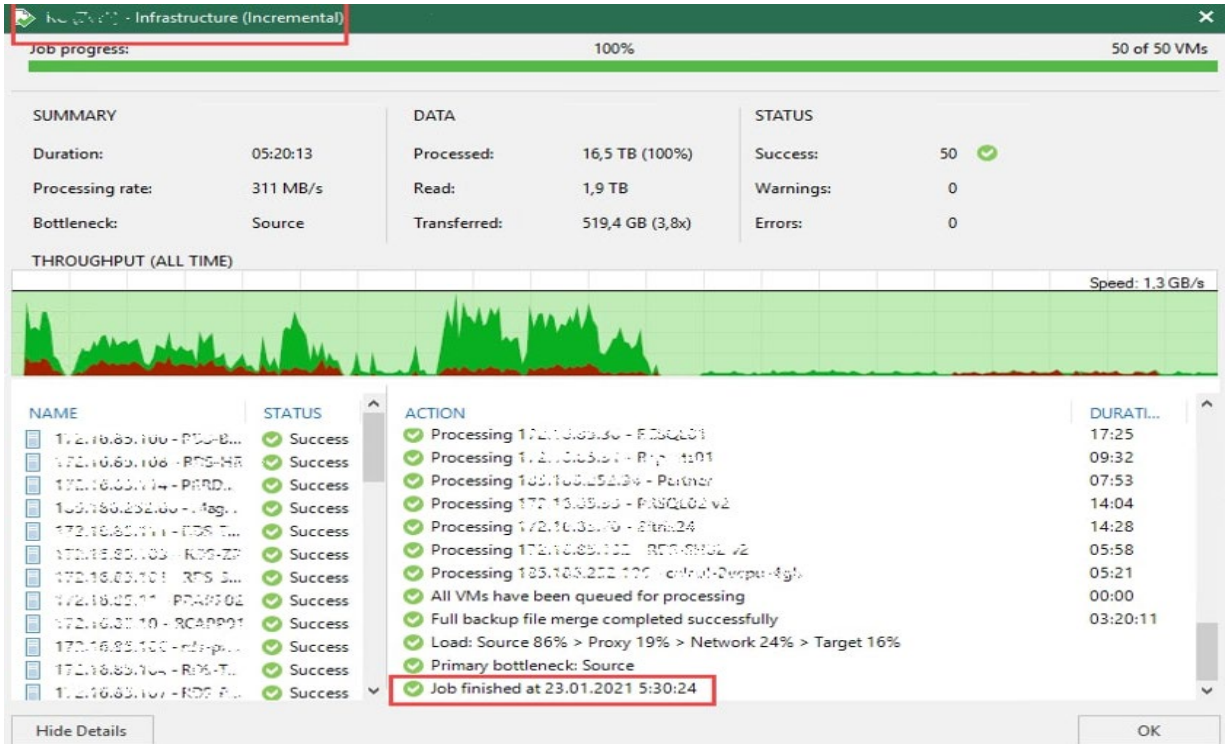


Рисунок 2.3 – Скріншот системи резервного копіювання Veeam

Основною причиною витоку корпоративних даних є неінформований персонал компанії – відвідування сумнівних сайтів та сервісів, перехід за посиланнями у спам та фішингових повідомленнях. Це також використання особистих телефонів, домашніх комп’ютерів для віддаленої роботи та інше.

Причиною компрометації облікових записів користувачів стають ненадійні паролі, використання однакових або стандартних паролів для соціальних мереж, сторонніх сервісів для роботи.

Коли компанія розподіляє доступи співробітників до своїх сервісів і не дотримується принципу «нульової довіри» виникають ситуації, коли будь-який співробітник (адміністратор, бухгалтер, менеджер), маючи відповідний логін та пароль, може зайти на будь-який корпоративний сервіс. Якщо обліковий запис такого співробітника вдасться скомпрометувати, то зловмисник матиме доступ взагалі до будь-якого сервісу.

До того ж, не у всіх компаній вистачає потужностей, щоби підтримати стабільну роботу корпоративних ресурсів при масі віддалених підключень. У

результаті - перехід на громадські послуги, передача робочих документів «для зручності» в месенджерах та соцмережах, зберігання даних у приватних хмарах. Усе це ризики випадкових чи навмисних витоків даних [17].

Враховуючи виклики сьогодення кожна компанія малого та середнього бізнесу повинна мати в своєму арсеналі базовий набір інструментів, комплекс засобів та дій для підвищення кіберзахисту, план оптимізації та рекомендації щодо усунення виявлених недоліків і вразливостей основних компонентів IT інфраструктури. Першим кроком до підвищення рівня кіберзахисту є системний аудит кібербезпеки – комплекс робіт з обстеження та виявлення вразливостей основних компонентів IT інфраструктури, розробка та виконання рекомендацій щодо їх усунення. В першу чергу необхідно провести обстеження та аналіз основних корпоративних систем і сервісів, а саме: мережева інфраструктура, серверна інфраструктура та система віртуалізації, служба каталогів AD, корпоративна пошта, системи резервного копіювання та моніторингу. Комплекс дій та технік, який представлено в таблиці 2.1, допоможе отримати реальну картину по мережеву та серверну складову IT інфраструктури , налаштування політик та правил безпеки, фільтрації, захисту від спаму, налаштовані метрики та оповіщення, забезпечення відмовостійкості та можливості відновлення роботи IT сервісів, виявити вразливості та розробити необхідні рекомендації з підвищення рівня безпеки [19].

Таблиця 2.1

Перелік базових тактик та технік аудиту кібербезпеки для основних компонентів IT інфраструктури SMB сегменту

Тактика	**Техніки**
Обстеження та виявлення вразливостей мережевої інфраструктури	Збір та аналіз загальної інформації про мережеву інфраструктуру
	Сканування мережевого обладнання за допомогою спеціалізованого програмного забезпечення автоматичного пошуку вразливостей

	Збір інформації щодо завантаження мережевих пристроїв за допомогою спеціалізованого програмного забезпечення, а також даних, що отримані із вбудованих функцій мережевого обладнання
	Аналіз мережевої інфраструктури в розрізі надійності та безпеки
Обстеження та виявлення вразливостей серверної інфраструктури	Збір та аналіз загальної інформації про серверну інфраструктуру
	Сканування серверного обладнання за допомогою спеціалізованого програмного забезпечення автоматичного пошуку вразливостей та наявності шкідливого ПЗ, первірка налаштувань брандмауера
	Перевірка застосованих політик AD на серверах і робочих станціях
	Оцінка актуальності оновлень ОС та антивірусного ПЗ
	Аналіз серверної інфраструктури в розрізі надійності та безпеки
Тестування на проникнення	Перевірка стійкості зовнішнього периметру до атак та проникнення
	Перевірка захисту внутрішньої мережі на предмет крадіжки або витоку інформації (у разі проникнення)
	Перевірка стійкості веб сайту до атак, спроба зупинити роботу ресурсу або підмінити тестову сторінку
	Збір та аналіз загальної інформації про поштову систему

Обстеження та виявлення вразливостей поштової системи	Перевірка налаштувань фільтрації, поштових записів та публікації клієнтського доступу
	Оцінка захисту поштової системи при отриманні шкідливих листів
	Перервірка та аналіз логування подій на поштовому сервері
	Аналіз поштової системи в розрізі надійності та безпеки
Обстеження та аналіз роботи системи моніторингу	Оцінка стану та аналіз функціональності
Обстеження та аналіз роботи системи резервного копіювання та відновлення	Оцінка стану та аналіз функціональності
Підготовка документації	Підготовка звіту з рекомендаціями по усуненню виявлених вразливостей та підвищенню рівня кіберзахисту основних компонентів IT інфраструктури.

Важливим елементом аудиту кібербезпеки є тестування на проникнення (penetration test).

Тестування на проникнення (пентест) – це метод оцінки стійкості корпоративної мережі до кіберзагроз. Під час пентесту команда фахівців з інформаційної безпеки, що діють в ролі хакерів, намагається зламати систему за попереднім погодженням з власником інформаційної системи.

Цілі пентесту полягають в наступному:

– У виявленні вразливостей: пентест допомагає знайти всі можливі вразливості в системі, які можуть бути використані хакерами для крадіжки даних, порушення роботи системи або вимагання викупу.

– У оцінці ризиків: на основі виявлених вразливостей фахівці з кібербезпеки можуть оцінити ризики для бізнесу та розробити план їх пом’якшення.

– У підвищенні стійкості: результати пентесту допомагають покращити захист корпоративної мережі та зробити її більш стійкою до кіберзагроз.

Існують кілька типів пентесту:

– Віртуальний пентест, що фокусується на тестуванні програмного забезпечення та мережевих ресурсів.

– Фізичний пентест, що фокусується на тестуванні фізичної безпеки, наприклад, намагаючись отримати несанкціонований доступ до приміщень або обладнання.

– Соціальний інжиніринг, що фокусується на тестуванні стійкості співробітників до соціальних методів маніпулювання, наприклад, фішингу або претекстових атак.

Хакери використовують інформацію про CMS, налаштування сервера та список скриптів, володіючи базовою інформацією про CMS, налаштування сервера та список скриптів, що використовуються на сайті, хакери можуть швидко знайти вже відомі вразливості, що значно полегшує їм процес проникнення. Цією можливістю користуються як хакери-початківці, так і більш досвідчені.

Переваги пентесту для SMB:

– Підвищення кібербезпеки: Пентест допомагає виявити та усунути вразливості до того, як ними скористаються хакери.

– Зниження ризиків: Пентест допомагає знизити ризики фінансових втрат, шкоди репутації та інших негативних наслідків кібератаки.

– Підвищення довіри: Пентест може допомогти підвищити довіру клієнтів та партнерів до вашого бізнесу, демонструючи вашу прихильність до кібербезпеки.

Отже, тестування на проникнення – це важливий інструмент, який може допомогти SMB захистити свої корпоративні мережі від кіберзагроз.

Впровадження пентесту може значно підвищити рівень кібербезпеки вашого бізнесу та знизити ризики кібератак.

Як показує практика, велика кількість веб-майстрів, що створюють сайти, не знають основних заходів безпеки при звичайному встановленню плагінів “за замовчуванням” на тому ж WordPress [18].

Моделювання дій кіберзлочинця – це метод оцінки стійкості корпоративної мережі до кібератак. Під час моделювання фахівці з кібербезпеки намагаються імітувати дії кіберзлочинця, щоб виявити вразливості та оцінити ризики для бізнесу.

Об’єкти, котрі перевіряються під час моделювання, представляють собою перш за все систему управління базами даних інформаційної системи: вона зберігає всі дані компанії, тому вона є однією з головних мішеней для кіберзлочинців. Також використовується мережеве обладнання, таке як маршрутизатори та комутатори, що може бути використано кіберзлочинцями для перехоплення трафіку або блокування доступу до ресурсів. Мережеві служби та сервіси, такі як електронна пошта, можуть бути використані кіберзлочинцями для розповсюдження шкідливого програмного забезпечення або фішингових атак.

Засоби захисту інформації, такі як брандмауери та антивірусне програмне забезпечення, можуть бути обійдені кіберзлочинцями, якщо вони мають відповідні знання та навички. Сервери часто містять цінні дані та ресурси, тому вони є привабливою мішенню для кіберзлочинців. Серверні та користувацькі операційні системи можуть містити вразливості, які можуть бути використані кіберзлочинцями для отримання доступу до системи.

Переваги моделювання дій кіберзлочинця для SMB:

- Підвищення кібербезпеки: Моделювання допомагає виявити та усунути вразливості до того, як ними скористаються кіберзлочинці.
- Зниження ризиків: Моделювання допомагає знизити ризики фінансових втрат, шкоди репутації та інших негативних наслідків кібератаки.
- Підвищення обізнаності: Моделювання може допомогти підвищити обізнаність співробітників про кіберзагрози та навчити їх протистояти їм.

Отже, моделювання дій кіберзлочинця - це важливий інструмент, який може допомогти SMB захистити свої корпоративні мережі від кібератак. Впровадження моделювання може значно підвищити рівень кібербезпеки вашого бізнесу та знизити ризики кібератак.

Для проведення пентесту та аудиту кібербезпеки вцілому малим та середнім компаніям рекомендується використовувати стандарти, засоби та базові програмні інструменти, які вказані в таблиці 2.2.

Таблиця 2.2

Інструменти та засоби для виявлення вразливостей та підвищення рівня кіберзахисту

Загальна система оцінки вразливостей Common Vulnerability Scoring System (CVSS)	Відкритий галузевий стандарт оцінки серйозності вразливостей безпеки системи та мереж, який може призначити градацію серйозності вразливостям, що дозволяє фахівцям, відповідно до загроз розподіляти пріоритети реагування
Сканер автоматичного пошуку вразливостей Tenable Nessus Vulnerability asessment	Найбільш поширений інструмент віддаленого сканування безпеки, який сканує обладнання, програми або віртуальні ресурси та надає інформацію, якщо виявляє вразливості, які зловмисники можуть використати, щоб отримати доступ до будь-якого обладнання, хмарного чи мережевого ресурсу
Сканер Microsoft Safety Scanner	Утиліта, яка сканує та перевіряє систему на наявність шкідливого ПЗ та вірусів, дозволяє виявляти загрози в системі без необхідності встановлення додаткового спеціалізованого ПЗ
Система моніторингу Zabbix	Повнофункціональне рішення моніторингу продуктивності та безпеки, оповіщення та сигналізації

Система резервного копіювання Veeam Backup & Replication	Програма резервного копіювання для віртуальних середовищ, побудованих на різних гіпервізорах
Платформа Kali Linux	Платформа для дослідження, аналізу та тестування на проникнення. Містить необхідний функціонал, який дає змогу спеціалістам з кібербезпеки виявляти й усувати різного роду вразливості
Сканер доменів та визначення IP адрес DNSmap	Інструмент призначений для використання пентестерами на етапі збору/перерахування інформації, виявлення мережевих IP-блоків, доменних імен, пошуку піддоменів
Мережевий сканер Nmap	Інструмент для сканування мережі та визначення відкритих портів і активних служб, для перевірки стану безпеки, ідентифікації ОС та додатків, типу файєрволу на вузлі,який сканується
Комплекс Metasploit	Дане програмне забезпечення використовується для спроби експлуатації виявлених загроз та вразливостей у системах та мережах
Сканер OWASP ZAP	Бататоцільовий інструмент сканування веб додатків
Сканер JoomScan	Інструмент для сканування веб-сайтів

2.3 Управління вразливостями

Одним з найважливіших елементів захисту інформації є управління вразливостями, адже кількість кіберінцидентів невпинно зростає. Методики до управління вразливостями можуть досить різноманітними, але їх об’єднує спільна ціль мету — зменшення ризиків пошкодження інформації чи її втрата. Отже, детальніше розкриємо та дамо рекомендації по збільшенню захисту IT

інфраструктури малих та середніх підприємств завдяки налагодженню процесу управління вразливостями, тому що сце є важливою складовою ефективності системи кіберзахисту компаній будь яких галузей в процесі цифрової трансформації. Для зменшення негативних наслідків організації повинні проводити системну роботу з управління вразливостями, а саме:

1. Підготувати та впровадити відповідні політики та план реагування на кіберінциденти.
2. Проводити інвентаризацію активів та системно намагатися оцінювати ризики, які з ними пов’язані.
3. Намагатися системно виявляти актуальні вразливості, слідкувати за змінами та новими техніками, методами експлуатації, оцінювати потенційні загрози щоб концентруватися на найбільш важливих та проблемних вразливостях, які несуть найбільшу небезпеку та ризик.
4. Необхідно постійно вдосконалювати програму керування вразливостями, слідкувати за змінами в інфраструктурі та розвитком загроз.

Основні етапи процесу управління вразливостями представлені на рисунку 2.4.

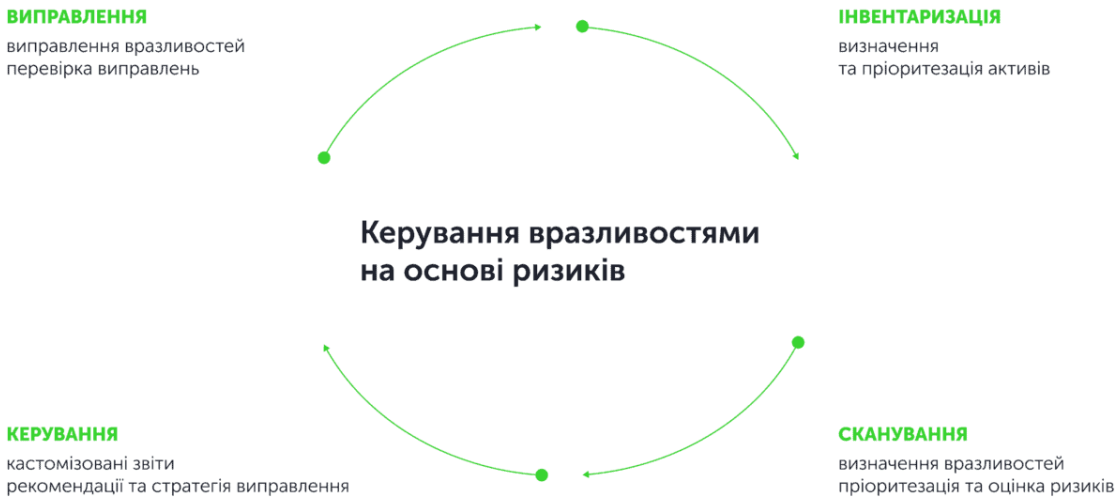


Рисунок 2.4 – Основні етапи управління процесу вразливостями

Важливо розуміти, що керування вразливостями — це системна операція, адже інформація про нові вразливості знінюється кожну добу. Вразливості виявляють за допомогою таких інструментів, як різноманітні сканери мережі, вебдодатків, виявлення вразливостей на обладнанні віддалених співробітників. Після виявлення - вразливості потрібно проаналізувати і надати їм відповідний пріорітет згідно ступеню ризику, що вони становлять. Для цього використовуються, наприклад, стандарт CVSS, який дозволяє оцінити серйозність по 10 бальній шкалі. Проте зараз, для більш ефективного використання ресурсів та зменшення вірогідності пропуску справді критичних вразливостей, також використовується метод управління на основі ризиків з використанням машинного навчання, що дозволяє збільшити обробку великої кількості даних, розуміти прецеденти використання та складність вразливості, активність зловмисників та відстеження їх ресурсів [20].

Компанія повинна враховувати та намагатись оцінювати максимум шляхів атак, якими зловмисники можуть проникнути в інформаційну систему. Важливо, при оцінці поверхні атаки, враховувати всі можливі активи: мережеві, серверні, бази даних, ПЗ, веб-додатки, тому що кожен з них може бути вразливим і стати вікном проникнення.

Збільшення точності визначення загроз відбувається за рахунок оцінки вразливостей всіх активів та їх зв’язків. Завдяки цьому організації можуть встановлювати відповідні пріорітети та приймають найбільш ефективні рішення з питань кіберзахисту. Встановлення пріорітетів усунення вразливостей та визначення критичності активів для бізнесу відбувається за рахунок розуміння конктесту відповідного активу та його зв’язків з іншими. Ідентифікація та класифікація всіх інформаційних активів та вразливостей, що з ними пов’язані – в цьому полягає основа оцінки поверхні атаки, основними етапами якої є:

1. Інвентаризація активів компанії, яка включає обладнання, ПЗ, мережеві ресурси, веб додатки, бази даних.

2. Визначення пріоритетів інформаційних активів, які назначаються відповідно до критичності та впливу на бізнес процеси та місця в інфраструктурі підприємства.

3. Організація системи зв’язку між активами, які можуть мати вплив один на одного.

4. Оцінка ризиків за допомогою відповідної системи класифікації чи стандарту, що допоможе оцінити ймовірність та наслідки атаки, а також визначити потенційні загрози.

5. Створення плану дій з мінімізації ризиків.

Для досягнення максимального ефекту в управлінні вразливостями необхідно:

– Системне навчання користувачів та підвищення рівня кібергігієни.

– Підтримка відповідних політик в актуальному стані, системне виконання процедури виявлення, опрацювання та усунення вразливостей.

– Постійне вдосконалення основних компонентів ІТ інфраструктури, підвищення та використання заходів захисту на рівні операційної системи, ПЗ, мкережевих ресурсів.

– Системне та вчасне оновлення ПЗ від вендорів та максимальне використання антивірусного ПЗ.

– Надійні паролі та їх систематична зміна.

– Обмеження та контроль прав та доступу користувачів.

– Мережева фільтрація трафіку задля запобігання проникнення та організація системи моніторингу.

– Створення та збереження актуальних резервних копій даних на постійній основі.

Управління вразливостями — необхідний компонент захисту інфраструктури компанії. Забезпечення захисту та запобігання кіберзагрозам, збереження даних відбувається завдяки реалізації відповідних заходів, проактивному виявленню, системному моніторингу та аналізу всієї поверхні атаки.

2.4 Висновки до другого розділу

В результаті підготовки другого розділу роботи розглянуті основні організаційні заходи по підвищенню рівня кіберзахисту на підприємствах малого та середнього сегменту.

Маючи набір інструментів та комплекс дій по виявленню вразливостей основних компонентів IT інфраструктури у SMB компаній є можливість вчасно виявляти вразливості та намагатися управляти ними, таким чином підвищуючи кіберзахист та збереження даних.

РОЗДІЛ 3
ВИЯВЛЕННЯ ВРАЗЛИВОСТЕЙ ТА РОЗРОБКА РЕКОМЕНДАЦІЙ З ПІДВИЩЕННЯ РІВНЯ КІБЕРЗАХИСТУ ІТ ІНФРАСТРУКТУРИ ТИПОВОЇ SMB КОМПАНІЇ

3.1 Обстеження, аналіз та виявлення вразливостей мережевої інфраструктури

В межах даного розділу розглянуто практичне застосування організаційних заходів, набору інструментів та комплексу дій по виявленню вразливостей основних компонентів ІТ інфраструктури на прикладі реалізації проекту аудиту кібербезпеки, розробимо рекомендації з підвищення рівня кібехзахисту для типової компанії SMB сегменту.

В рамках даного проекту було проведено:

– базовий міні-тренінг для керівництва та ІТ адміністраторів з основ кібергігієни, надані необхідні матеріали та настанови для організації та проведененя в майбутньому системних інструктажів для всіх співробітників організації;

– збір і аналіз інформації про основні компоненти ІТ інфраструктури, а саме про мережеву інфраструктуру, бездротову мережу, серверну інфраструктуру (включаючи обстеження робочих станцій) і системи віртуалізації, службу Active Directory і поштову систему, веб-сайт, системи моніторингу, резервного копіювання та відновлення;

– аналіз основних компонентів ІТ інфраструктури в розрізі надійності і безпеки: тестування захищеності ІТ сервісів з точки зору інформаційної безпеки (тестування на проникнення);

– розробку рекомендацій з підвищення рівня кібехзахисту та інформаційної безпеки.

Інформаційна корпоративна система типової компанії малого та середнього бізнесу складається з єдиної мережі підприємства. Серверна і мережева інфраструктура організовані на базі наступних вендорів: Cisco, HP, Supermicro, Microsoft, Mikrotik, Sophos. На підприємстві заходиться 1 (один) основний центр комутації та 3 (три) проміжні центри комутації, які знаходяться в різних промислових приміщення. Комутація з проміжних центрів комутації зводиться в основний центр комутації. Мережева інфраструктура компанії складається з такого обладнання:

1. Маршрутизатор-файервол Sophos UTM9 SG135
2. Комутатор рівня ядра Cisco 3750G-48
3. Комутатор рівня агрегації Cisco 3750-12S
4. Комутатор Cisco SF200 (в центрі комутації 1)
5. Комутатор Cisco 2960G-24 (в центрі комутації 2)
6. Комутатор Cisco 2960G-24 (в центрі комутації 3)
7. Точка доступу Ubiquiti 4
8. Точка доступу Ubiquiti 5
9. Точка доступу Dlink DIR-300
10. Комутатор Mikrotik CRS112-8G-4S (виконує роль комутатора рівня доступу)
11. Комутатор Mikrotik RB-751U (виконує роль комутатора рівня доступу)
12. Комутатор Mikrotik RB-951U (виконує роль комутатора рівня доступу)

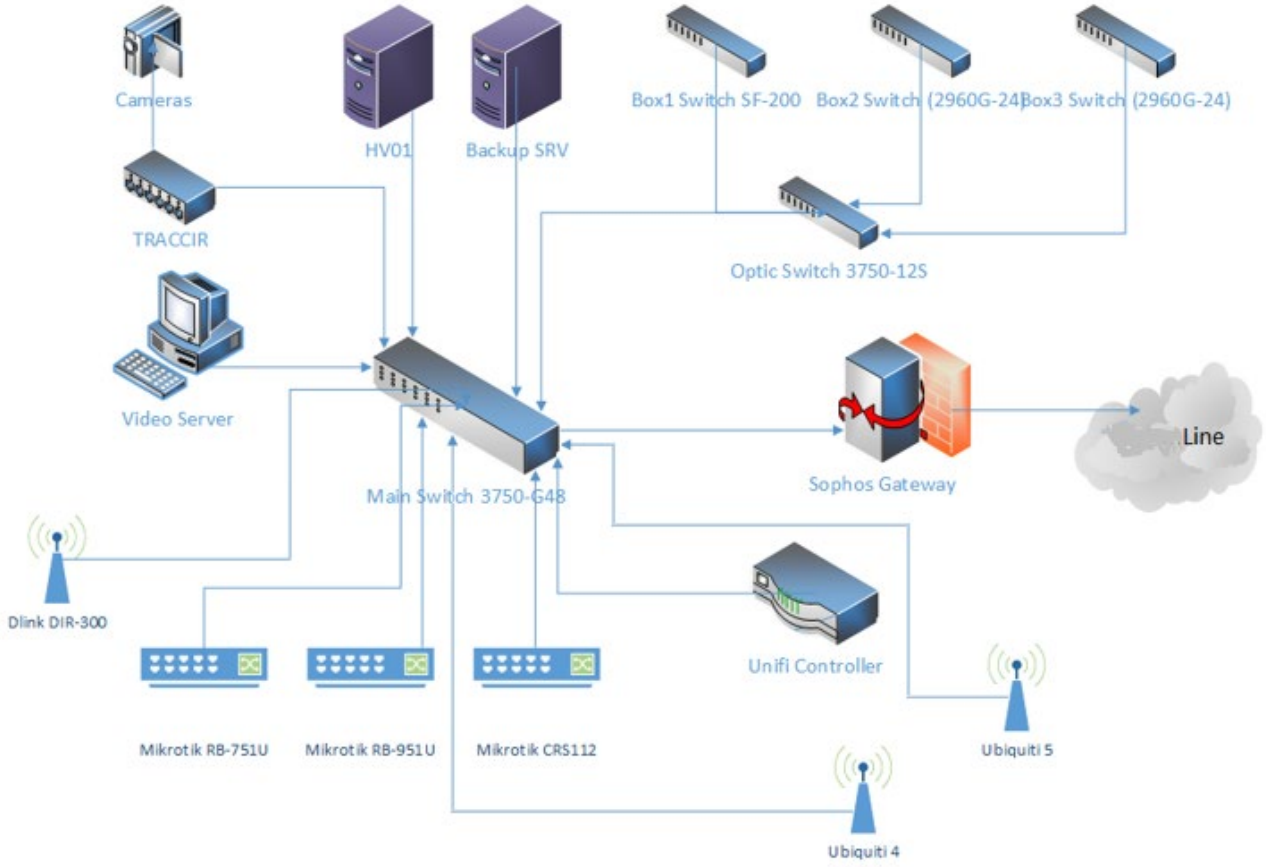


Рисунок 3.1 – Загальна схема мережі SMB підприємства

В ході обстеження та аналізу мережі підприємства було проведено:

– сканування мережевих пристроїв за допомогою спеціалізованого інструменту автоматичного пошуку вразливостей Tenable Nessus Vulnerability asessment v8.14, в якому перелік та класифікація вразливостей наведені відповідно до стандарту CVSSv2.0).

– отримано інформацію щодо завантаження мережевих пристроїв за допомогою системи моніторингу Zabbix v3.4.9, а також даних, що отримані із вбудованих функцій мережевого обладнання.

1. Маршрутизатор-файервол Sophos UTM9 SG135

Проведено автоматизоване сканування Sophos UTM9 SG135 системою пошуку вразливостей:

Рисунок 3.2 – Результат пошуку вразливостей на Sophos UTM9 SG135

В результаті проведення автоматизованого сканування в програмному заберпеченні Sophos UTM9 SG135 не виявлено вразливих елементів.

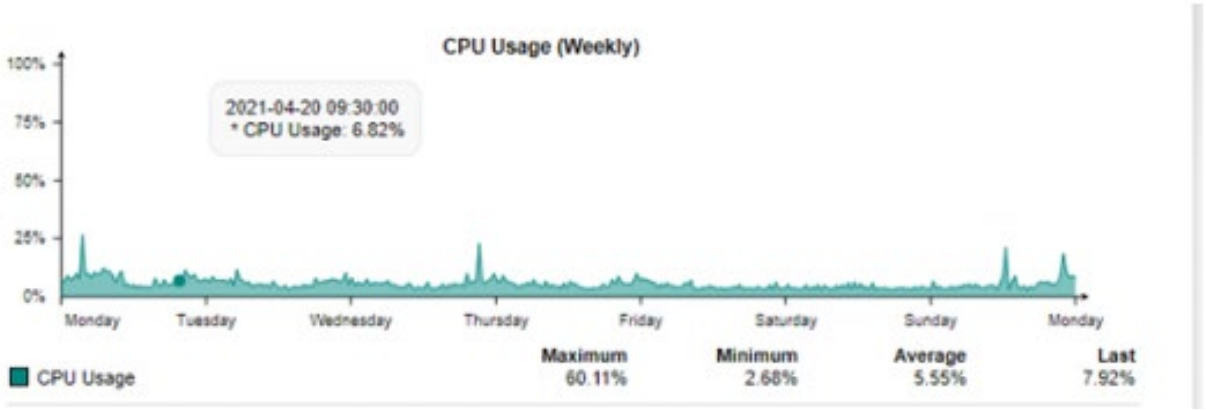


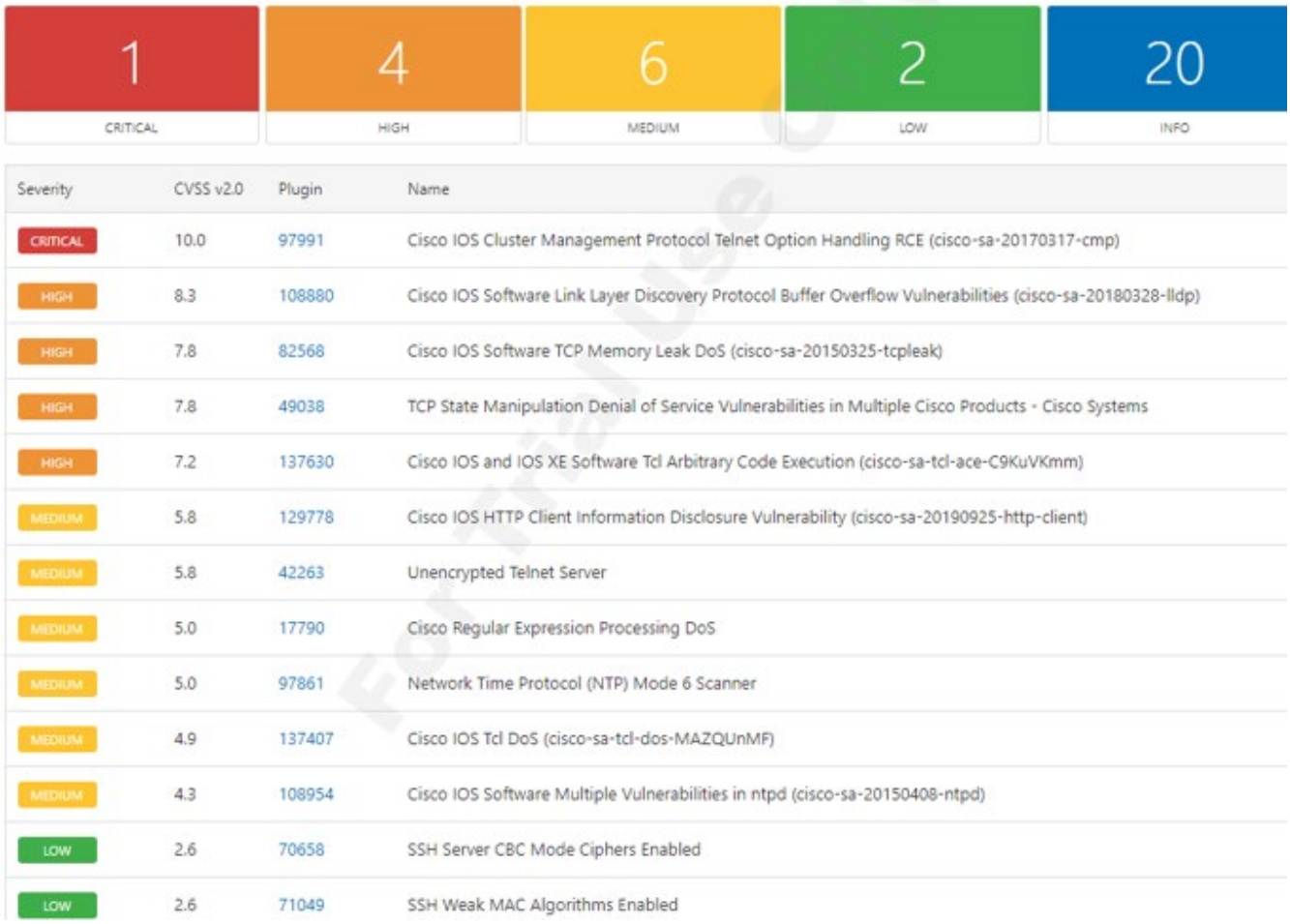
Рисунок 3.3 - Навантаження на центральному процесорі Sophos UTM9 SG135

Навантаження на центральний процесор, оперативну пам’ять, дисковий простір та мережевий інтерфейс на Sophos UTM9 SG135 є допустимими, а на

самому пристрої не було знайдено критичних вразливостей. Враховуючи, що даний пристрій є міжмережевим шлюзом та єдиною можливою точкою проникнення до мережі ззовні (без використання методів соціальної інженерії) - зовнішній периметр вважаємо захищеним.

2. Комутатор рівня ядра Cisco 3750G-48

В результаті проведення автоматизованого сканування на вразливості в програмному забезпеченні комутатора Cisco 3750G-48 було виявлено наступний перелік вразливостей різного ступеню критичності:



1	4	6	2	20
CRITICAL	HIGH	MEDIUM	LOW	INFO

Severity	CVSS v2.0	Plugin	Name
CRITICAL	10.0	97991	Cisco IOS Cluster Management Protocol Telnet Option Handling RCE (cisco-sa-20170317-cmp)
HIGH	8.3	108880	Cisco IOS Software Link Layer Discovery Protocol Buffer Overflow Vulnerabilities (cisco-sa-20180328-lldp)
HIGH	7.8	82568	Cisco IOS Software TCP Memory Leak DoS (cisco-sa-20150325-tcpleak)
HIGH	7.8	49038	TCP State Manipulation Denial of Service Vulnerabilities in Multiple Cisco Products - Cisco Systems
HIGH	7.2	137630	Cisco IOS and IOS XE Software Tcl Arbitrary Code Execution (cisco-sa-tcl-ace-C9KuVKmm)
MEDIUM	5.8	129778	Cisco IOS HTTP Client Information Disclosure Vulnerability (cisco-sa-20190925-http-client)
MEDIUM	5.8	42263	Unencrypted Telnet Server
MEDIUM	5.0	17790	Cisco Regular Expression Processing DoS
MEDIUM	5.0	97861	Network Time Protocol (NTP) Mode 6 Scanner
MEDIUM	4.9	137407	Cisco IOS Tcl DoS (cisco-sa-tcl-dos-MAZQUnMF)
MEDIUM	4.3	108954	Cisco IOS Software Multiple Vulnerabilities in ntpd (cisco-sa-20150408-ntpd)
LOW	2.6	70658	SSH Server CBC Mode Ciphers Enabled
LOW	2.6	71049	SSH Weak MAC Algorithms Enabled

Рисунок 3.4 - Перелік та класифікація виявлених вразливостей Cisco 3750G-48

Виявлена критична вразливість, що дозволяє неаутентифікованому користувачу встановити сеанс Telnet для виконання шкідливого коду за умови знаходження всередині мережі. Виявлені вразливості, тим не менш, не можуть бути

використані для проникнення до мережі ззовні і можуть бути використані тільки у випадку, якщо зловмисник знаходиться всередині мережі.

За допомогою системи моніторингу були зняті показники рівнів завантаженості центрального процесора, оперативної пам’яті, мережевих інтерфейсів.

Під найбільшим навантаженням наступні мережеві інтерфейси: інтерфейс Gi1/0/34, інтерфейс Gi1/0/49, інтерфейс Gi1/0/50, інтерфейс Po1.

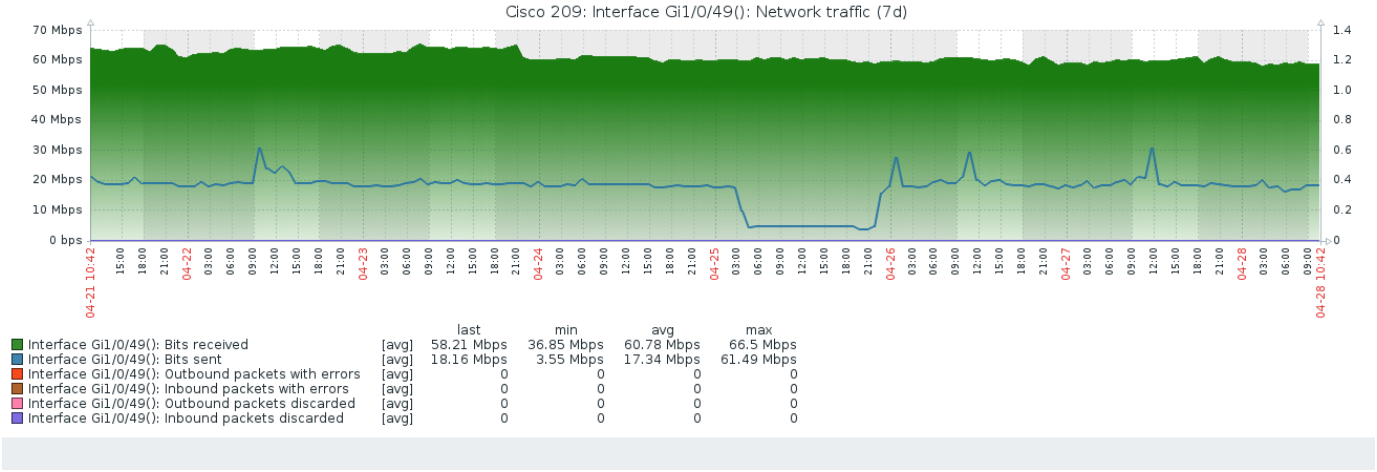
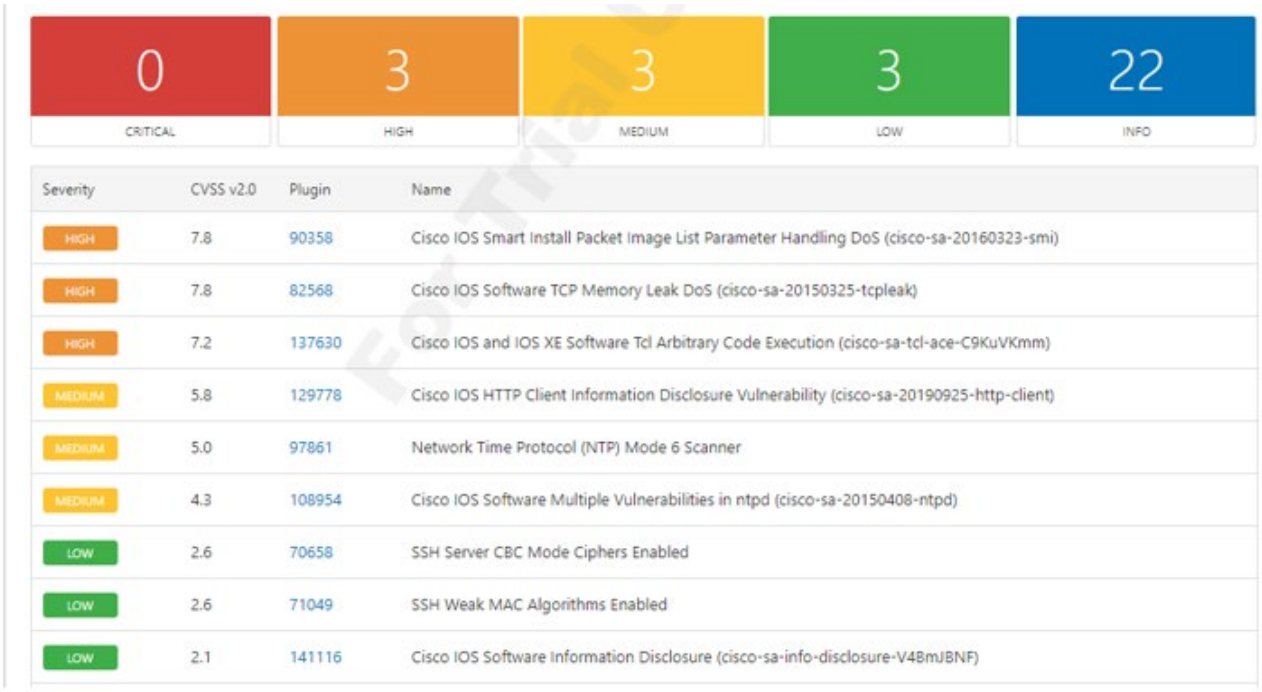


Рисунок 3.5 - Завантаженість мережевого інтерфейсу Gi1/0/49 Cisco 3750G-48

Відповідно до звіту системи моніторингу, завантаженість обладнання знаходиться на середньому рівні і в пікових ситуаціях не перевищує критичних значень.

3. Комутатор рівня агрегації Cisco 3750-12S

В результаті проведення автоматизованого сканування на вразливості в програмному забезпеченні Cisco 3750-12S було виявлено наступний перелік вразливостей різного ступеню критичності:



0	3	3	3	22
CRITICAL	HIGH	MEDIUM	LOW	INFO

Severity	CVSS v2.0	Plugin	Name
HIGH	7.8	90358	Cisco IOS Smart Install Packet Image List Parameter Handling DoS (cisco-sa-20160323-smi)
HIGH	7.8	82568	Cisco IOS Software TCP Memory Leak DoS (cisco-sa-20150325-tcpleak)
HIGH	7.2	137630	Cisco IOS and IOS XE Software Tcl Arbitrary Code Execution (cisco-sa-tcl-ace-C9KuVKmm)
MEDIUM	5.8	129778	Cisco IOS HTTP Client Information Disclosure Vulnerability (cisco-sa-20190925-http-client)
MEDIUM	5.0	97861	Network Time Protocol (NTP) Mode 6 Scanner
MEDIUM	4.3	108954	Cisco IOS Software Multiple Vulnerabilities in ntpd (cisco-sa-20150408-ntpd)
LOW	2.6	70658	SSH Server CBC Mode Ciphers Enabled
LOW	2.6	71049	SSH Weak MAC Algorithms Enabled
LOW	2.1	141116	Cisco IOS Software Information Disclosure (cisco-sa-info-disclosure-V4BmJBNF)

Рисунок 3.5 - Перелік та класифікація виявлених вразливостей Cisco 3750-12S

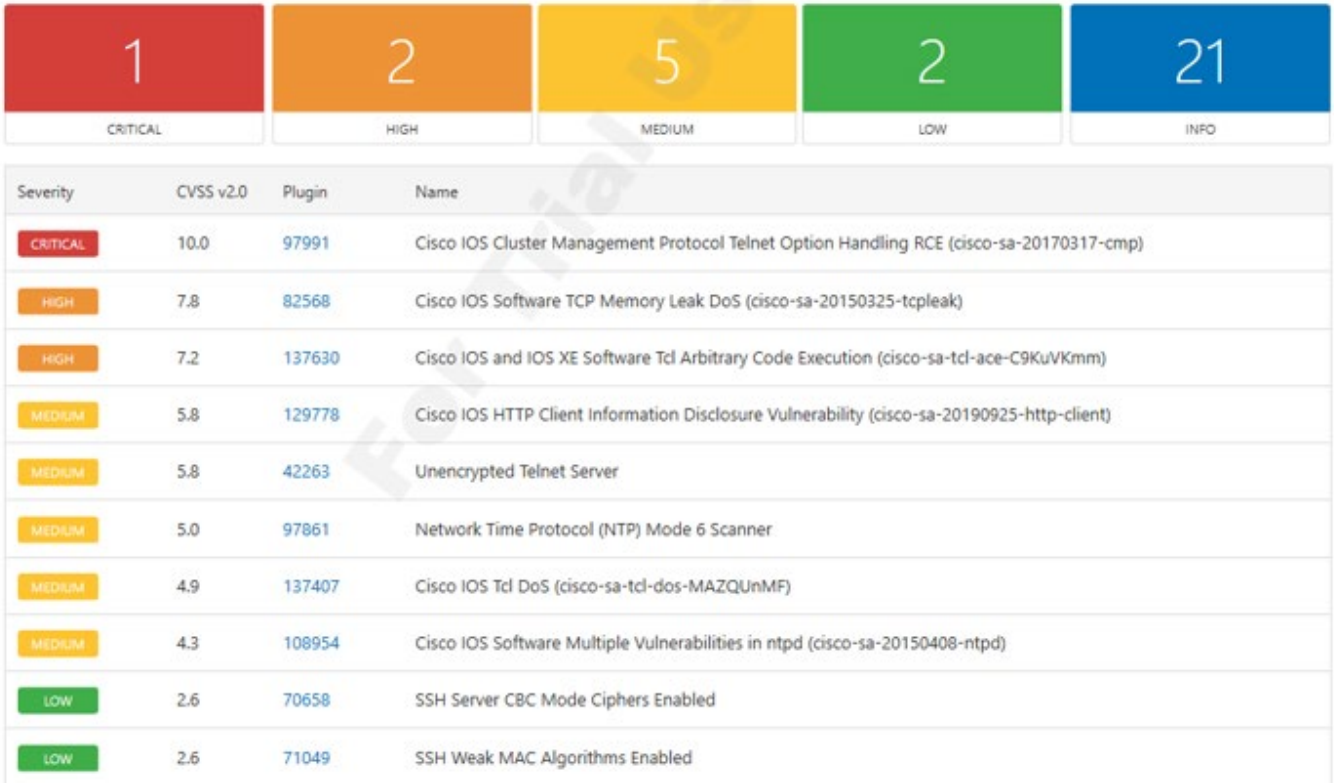
За допомогою системи моніторингу були зняті показники рівнів завантаженості центрального процесора, оперативної пам’яті, мережевих інтерфейсів - завантаженість обладнання знаходиться на середньому рівні і в пікових ситуаціях не перевищує критичних значень.

4. Комутатори Cisco SF200 (в центрі комутації 1) та Cisco 2960G-24 (в центрі комутації 2).

В результаті проведення автоматизованого сканування на вразливості в програмному забезпеченні цих комутаторів виявлено певний перелік вразливостей різного ступеню критичності, згідно даних системи моніторингу завантаженість обладнання знаходиться на середньому рівні і в пікових ситуаціях не перевищує критичних значень. Через те, що Cisco SF200 є застарілим обладнанням, немає можливості зняти значення завантаженості центрального процесора та оперативної пам’яті.

5. Комутатор Cisco 2960G-24 (в центрі комутації 3).

В результаті проведення автоматизованого сканування на вразливості в програмного забезпечення Cisco 2960G-24 було виявлено наступний перелік вразливостей різного ступеню критичності:



1	2	5	2	21
CRITICAL	HIGH	MEDIUM	LOW	INFO

Severity	CVSS v2.0	Plugin	Name
CRITICAL	10.0	97991	Cisco IOS Cluster Management Protocol Telnet Option Handling RCE (cisco-sa-20170317-cmp)
HIGH	7.8	82568	Cisco IOS Software TCP Memory Leak DoS (cisco-sa-20150325-tcpleak)
HIGH	7.2	137630	Cisco IOS and IOS XE Software Tcl Arbitrary Code Execution (cisco-sa-tcl-ace-C9KuVKmm)
MEDIUM	5.8	129778	Cisco IOS HTTP Client Information Disclosure Vulnerability (cisco-sa-20190925-http-client)
MEDIUM	5.8	42263	Unencrypted Telnet Server
MEDIUM	5.0	97861	Network Time Protocol (NTP) Mode 6 Scanner
MEDIUM	4.9	137407	Cisco IOS Tcl DoS (cisco-sa-tcl-dos-MAZQUnMF)
MEDIUM	4.3	108954	Cisco IOS Software Multiple Vulnerabilities in ntpd (cisco-sa-20150408-ntpd)
LOW	2.6	70658	SSH Server CBC Mode Ciphers Enabled
LOW	2.6	71049	SSH Weak MAC Algorithms Enabled

Рисунок 3.6 - Перелік та класифікація виявлених вразливостей Cisco 2960G-24

Виявлена критична вразливість дозволяє неаутентифікованому користувачу встановити сеанс Telnet для виконання шкідливого коду за умови знаходження все редині мережі.

За допомогою системи моніторингу були зняті показники рівнів завантаженості центрального процесора, оперативної пам’яті, мережевих інтерфейсів - завантаженість обладнання знаходиться на середньому рівні і в пікових ситуаціях не перевищує критичних значень.

6. Точки доступу Ubiquiti (4,5) та Dlink DIR-300

В результаті проведення автоматизованого сканування на вразливості в програмному забезпеченні цих точок доступу виявлено певний перелік вразливостей різного ступеню критичності, згідно даних системи моніторингу

завантаженість обладнання знаходиться на середньому рівні і в пікових ситуаціях не перевищує критичних значень. Через те, що точка доступу Dlink DIR-300 є застарілим обладнанням - вона фізично не підтримує можливість зняття даних системою моніторингу.

7. Комутатори рівня доступу Mikrotik CRS112-8G-4S, Mikrotik RB-751U, Mikrotik RB-951U.

В результаті проведення автоматизованого сканування на вразливості в програмному забезпечені комутатора Mikrotik CRS112-8G-4S було виявлено певний перелік вразливостей різного ступеню критичності. Відповідно до звіту системи моніторингу завантаженість цього комутатора знаходиться на середньому рівні і в пікових ситуаціях не перевищує критичних значень. Мережеві інтерфейси не перевантажені, однак слід звернути увагу на інтерфейс ether8, навантаження на якому дещо збільшене.

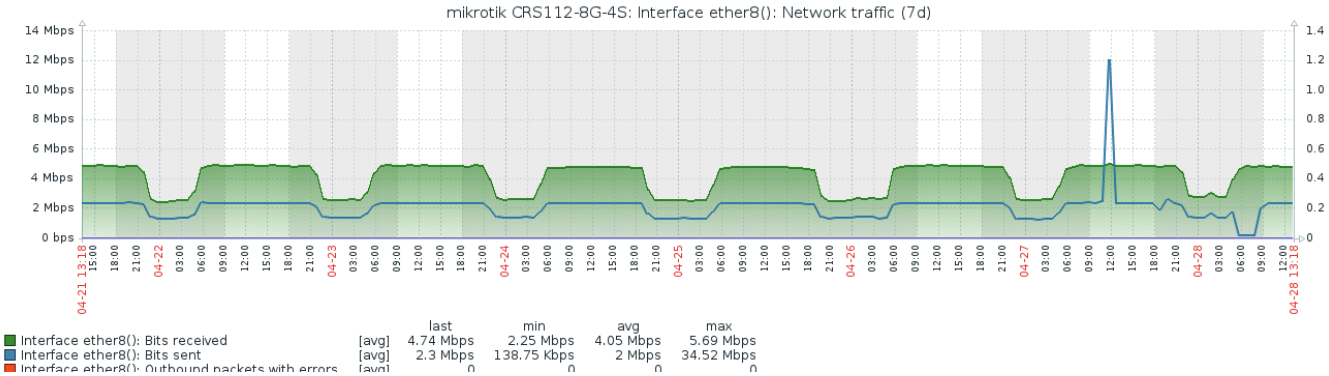
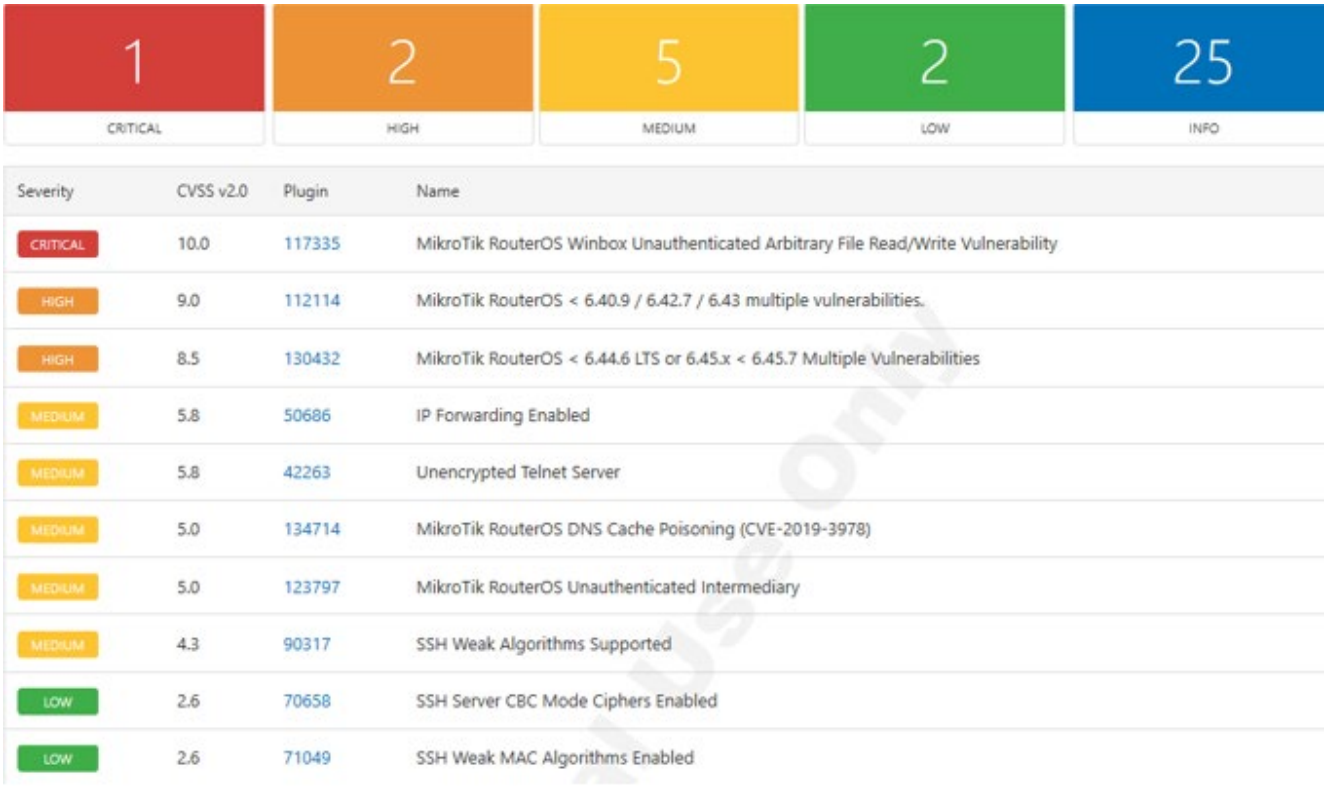


Рисунок 3.7 - Завантаженість мережевого інтерфейсу ether8 Mikrotik CRS112-8G-4S

В результаті проведення автоматизованого сканування на вразливості в програмному забезпечені комутатора Mikrotik RB-751U виявлена критична вразливість, яка дозволяє неавторизованому користувачу (за умови, якщо такий користувач знаходиться всередині мережі) проводити читання/запис файлів хосту, що може спричинити збої в системі, встановлення та змінення конфігурації обладнання.



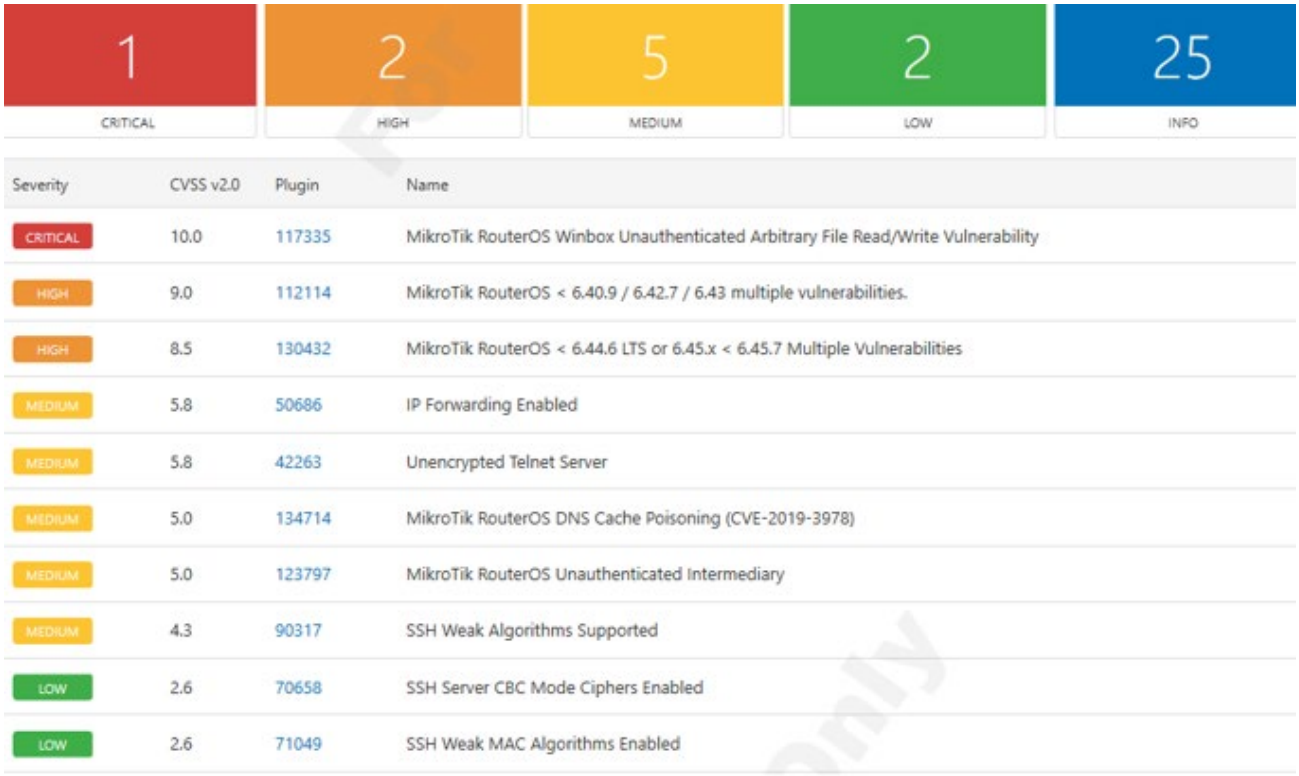
1	2	5	2	25
CRITICAL	HIGH	MEDIUM	LOW	INFO

Severity	CVSS v2.0	Plugin	Name
CRITICAL	10.0	117335	MikroTik RouterOS Winbox Unauthenticated Arbitrary File Read/Write Vulnerability
HIGH	9.0	112114	MikroTik RouterOS < 6.40.9 / 6.42.7 / 6.43 multiple vulnerabilities.
HIGH	8.5	130432	MikroTik RouterOS < 6.44.6 LTS or 6.45.x < 6.45.7 Multiple Vulnerabilities
MEDIUM	5.8	50686	IP Forwarding Enabled
MEDIUM	5.8	42263	Unencrypted Telnet Server
MEDIUM	5.0	134714	MikroTik RouterOS DNS Cache Poisoning (CVE-2019-3978)
MEDIUM	5.0	123797	MikroTik RouterOS Unauthenticated Intermediary
MEDIUM	4.3	90317	SSH Weak Algorithms Supported
LOW	2.6	70658	SSH Server CBC Mode Ciphers Enabled
LOW	2.6	71049	SSH Weak MAC Algorithms Enabled

Рисунок 3.8 - Перелік та класифікація виявлених вразливостей Mikrotik RB-751U

Відповідно до звіту системи моніторингу завантаженість цього комутатора знаходиться на середньому рівні і в пікових ситуаціях не перевищує критичних значень.

В результаті проведення автоматизованого сканування на вразливості в програмному забезпечені комутатора Mikrotik RB-951U було виявлено наступний перелік вразливостей різного ступеню критичності. Виявлена критична вразливість, яка дозволяє неавторизованому користувачу (за умови, якщо такий користувач знаходиться всередині мережі) проводити читання/запис файлів хосту, що може спричинити збої в системі, встановлення та змінення конфігурації обладнання. Відповідно до звіту системи моніторингу завантаженість цього комутатора знаходиться на середньому рівні і в пікових ситуаціях не перевищує критичних значень.



1	2	5	2	25
CRITICAL	HIGH	MEDIUM	LOW	INFO

Severity	CVSS v2.0	Plugin	Name
CRITICAL	10.0	117335	MikroTik RouterOS Winbox Unauthenticated Arbitrary File Read/Write Vulnerability
HIGH	9.0	112114	MikroTik RouterOS < 6.40.9 / 6.42.7 / 6.43 multiple vulnerabilities.
HIGH	8.5	130432	MikroTik RouterOS < 6.44.6 LTS or 6.45.x < 6.45.7 Multiple Vulnerabilities
MEDIUM	5.8	50686	IP Forwarding Enabled
MEDIUM	5.8	42263	Unencrypted Telnet Server
MEDIUM	5.0	134714	MikroTik RouterOS DNS Cache Poisoning (CVE-2019-3978)
MEDIUM	5.0	123797	MikroTik RouterOS Unauthenticated Intermediary
MEDIUM	4.3	90317	SSH Weak Algorithms Supported
LOW	2.6	70658	SSH Server CBC Mode Ciphers Enabled
LOW	2.6	71049	SSH Weak MAC Algorithms Enabled

Рисунок 3.9 - Перелік та класифікація виявлених вразливостей Mikrotik RB-951U

В цілому, мережева інфраструктура є достатньо стійкою і безпечною, однак слід звернути особливу увагу на наступні аспекти:

1. Не реалізовано відмовостійкості на рівні обладнання, комутатор рівня ядра є єдиною точкою відмови, в результаті виходу з ладу якої може бути паралізовано роботу всієї мережі;
2. Не реалізовано альтернативні канали виходу в Інтернет;
3. Не реалізовано відмовостійкості на рівні обладнання, маршрутизатор-фаєрвол є єдиною точкою відмови, в результаті виходу з ладу якого може бути паралізовано роботу із мережею Інтернет;
4. Не налаштовано функцій логування на мережевому обладнанні. Використання централізованого збору файлів системних журналів (лог-файлів) дозволяє значно пришвидшити пошук і усунення несправностей, а також проводити кореляцію подій у мережі;

5. Клієнти, мережеве обладнання та сервери знаходяться в одній підмережі, що є потенційним ризиком у випадку злому обладнання та поширення вірусів;

6. На мережевому обладнанні використовується застарілі версії програмного забезпечення, в яких є уразливості;

7. На сервері моніторингу Zabbix використовуються стандартна комбінація логіна і пароля адміністратора, що є загрозою безпеки в плані можливості дослідження інфраструктури зловмисниками за допомогою системи моніторингу у разі проникнення;

8. Не реалізовано функцій L2-безпеки на комутаторах. Функції безпеки на канальному рівні дозволяють зменшити ризики і значно ускладнити дії зловмисника у випадку його проникнення всередину мережі;

9. Точки доступу/домашні маршрутизатори D-Link не мають достатнього рівня функціоналу, що дозволяв би їх ефективне, зручне і безпечне їх використання в мережах корпоративного рівня.

3.2 Обстеження, аналіз та виявлення вразливостей серверної інфраструктури та робочих станцій

Співробітники компанії використовують 35 робочих станцій на ОС Windows. Характеристики робочих станцій отримано за допомогою ПЗ AIDA64 та LanSweeper.

В організації присутні два фізичних сервери – сервер Supermicro та сервер HP ProLiant ML350. Сервер Supermicro використовується як основний сервер віртуалізації. На сервері встановлена операційна система Windows Server 2012R2 Datacenter (активована) з роллю Hyper-V. Сервер HP ProLiant ML350 використовується в якості бекапного серверу для виконання та збереження бекапів віртуальних машин. На сервері встановлена операційна система Windows Server 2012R2 Datacenter (не активована).

Обидва фізичні сервери - це двохпроцесорні системи 2013 року випуску.

Моніторинг інфраструктури виконується за за допомогою ПЗ VeeamOne 9.5 (ver. 9.5.0.3254) та ПЗ Zabbix (ver.3.4.9). VeeamOne - віртуальна машина, яка виконує моніторинг основного серверу віртуалізації та віртуальних серверів на данному хості. Сповіщення у системі моніторингу VeeamOne по SMTP протоколу не налаштовані. Попереджень та помилок у системі моніторингу на момент обстеження не виявлено.

Zabbix (ver.3.4.9) - віртуальна машина під управлінням ОС Linux, розташована на основному сервері віртуалізації. Дана система моніторингу використовується для зняття даних завантаження мережевого обладнання, а також може бути використана для моніторингу серверів та віртуальних машин.

Системи моніторингу VeeamOne та Zabbix на данний момент покриває моні торинг усієї серверної та мережевої інфраструктури. Сповіщення по SMTP працю є тільки на Zabbix. В інфраструктурі на деяких вузлах виявлено агенти SCOM, а також створена віртуальна машина SCOM (вимкнена).

Система резервного копіювання організована на фізичному серверу HP ProLiant ML350 G5. У якості ПЗ для виконання бекапів використовуєтся продукт Veeam Backup & Replication 9.0 (ver. 9.0.0.1715), який встановлено на операційну систему Windows Server 2012 R2 Datacenter (не активована). Для бекапного серверу доданий один репозиторій - локальний Raid 5 з трьох дисків (D:\Backup). Створено 7 (сім) завдань для виконання бекапів ключових віртуальних машин. Завдання налаштовані на зберігання 14 (чортирнадцяти) точок та періодичне створення синтетичного бекапу. Сповіщення про виконання робіт по SMTP протоколу не налаштоване. Завдання для виконання бекапу виконуются починаючи з 21:00. Останнє завдання запускається у нічний час у 03.45. Помилок та попереджень на бекапному сервері не виявлено.

За допомогою системи моніторингу Zabbix були зняті показники рівнів завантаженості центрального процесора, оперативної пам’яті, дискового простору на бекапному сервері HP ProLiant ML350. Сервер бекапів працює в межах норми. Запасу дисків для виконання бекапів вистачає.

На сервері Supermicro один мережевий інтерфейс Intel 82574L Gigabit Network Connection #2 не використовується. Створено два рейди: Raid 0, Raid 10. Raid 0 містить 1 SSD диск (фактично не є Raid 0) і використовується під операційну систему хоста віртуалізації. Raid 10 створений з 6 HDD - використовується під розміщення віртуальних машин хоста віртуалізації. Один диск позначений як гаряча заміна, фактично він зможе замінити один диск з Raid 10. Поштовий сервер для сповіщень з рейд контролера не задано.

За допомогою системи моніторингу VeeamOne були зняті показники рівнів завантаженості центрального процесора, оперативної пам’яті, мережевого інтерфейсу, дискового простору на хості віртуалізації Supermicro у розрізі одного тижня. Сервер Supermicro на момент обстеження витримує навантаження віртульних машин, але має вже граничне значення навантаження по оперативній пам’яті 70-90%.Подальше створення віртуальних машин для впровадження або підвищення відмовостійкості поточних сервісів може призвести до нестабільної роботи хоста віртуалізації та віртуальних серверів на ньому. Віртуальні сервери мають пряму залежність від навантаження та ресурсів хоста віртуалізації. Показники навантаження віртуальних серверів в рамках норми.

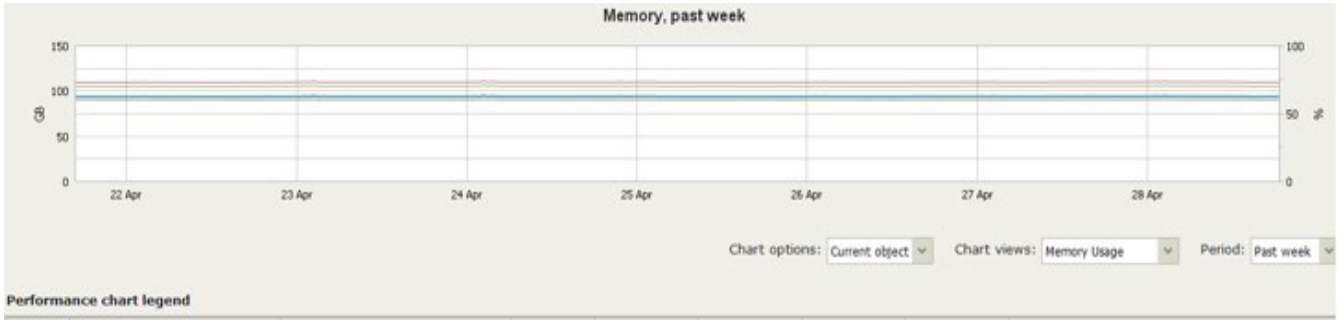


Рисунок 3.11 – Навантаження оперативної пам’яті на сервері Supermicro

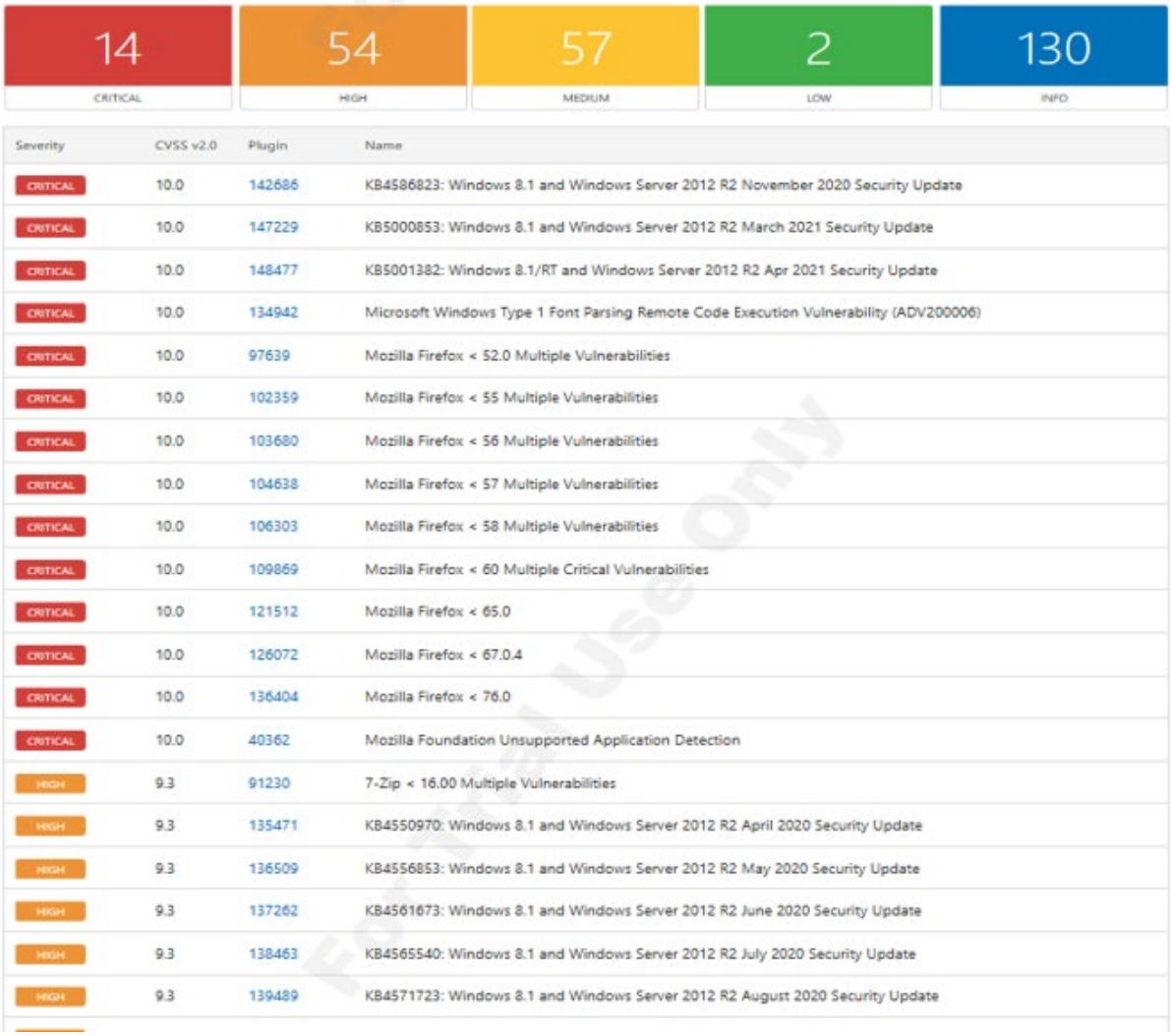
На сервері віртуалізації організовані віртуальні сервери з наступними характеристиками.

Таблиця 3.1

Характеристики віртуальних серверів на фізичному сервері Supermicro

Найменування	Операційна ситема	Статус	Кількість процесорів	Об’єм ОЗУ (Mb)	Об’єм диску (GB)
DC01	Windows Server 2012R2 std	Running	2	2048	40
Mail01-Exchange2016	Windows Server 2012R2 std	Running	6	24576	650
FS01	Windows Server 2012R2 std	Running	1	6144	250
UKRS02SQLV	Windows Server 2012R2 std	Running	8	24576	150
Customs-SRV	Windows Server 2012R2 std	Running	2	2048	50
TS01	Windows Server 2012R2 std	Running	4	6144	800
VeeamOne	Windows Server 2012R2 std	Running	4	4096	60
Zabbix	Windows Server 2012R2 std	Running	2	2048	20

В результаті проведення автоматизованого сканування на вразливості в програмному забезпеченні серверу віртуалізації Supermicro та бекапного серверу HP ProLiant ML350 було виявлено велику кількість вразливостей критичного ступеню, які можуть суттєво впливати на роботу IT сервісів компанії. Виявлені критичні вразливості, які за умови знаходження всередині мережі підприємства, можуть бути використані неавторизованим користувачем для доступа до даних, їх видалення, перехоплення паролів користувачів, зупинення та модифікації сервісів, програмного забезпечення.



14	54	57	2	130
CRITICAL	HIGH	MEDIUM	LOW	INFO

Severity	CVSS v2.0	Plugin	Name
CRITICAL	10.0	142686	KB4586823: Windows 8.1 and Windows Server 2012 R2 November 2020 Security Update
CRITICAL	10.0	147229	KB5000853: Windows 8.1 and Windows Server 2012 R2 March 2021 Security Update
CRITICAL	10.0	148477	KB5001382: Windows 8.1/RT and Windows Server 2012 R2 Apr 2021 Security Update
CRITICAL	10.0	134942	Microsoft Windows Type 1 Font Parsing Remote Code Execution Vulnerability (ADV200006)
CRITICAL	10.0	97639	Mozilla Firefox < 52.0 Multiple Vulnerabilities
CRITICAL	10.0	102359	Mozilla Firefox < 55 Multiple Vulnerabilities
CRITICAL	10.0	103680	Mozilla Firefox < 56 Multiple Vulnerabilities
CRITICAL	10.0	104638	Mozilla Firefox < 57 Multiple Vulnerabilities
CRITICAL	10.0	106303	Mozilla Firefox < 58 Multiple Vulnerabilities
CRITICAL	10.0	109869	Mozilla Firefox < 60 Multiple Critical Vulnerabilities
CRITICAL	10.0	121512	Mozilla Firefox < 65.0
CRITICAL	10.0	126072	Mozilla Firefox < 67.0.4
CRITICAL	10.0	136404	Mozilla Firefox < 76.0
CRITICAL	10.0	40362	Mozilla Foundation Unsupported Application Detection
HIGH	9.3	91230	7-Zip < 16.00 Multiple Vulnerabilities
HIGH	9.3	135471	KB4550970: Windows 8.1 and Windows Server 2012 R2 April 2020 Security Update
HIGH	9.3	136509	KB4556853: Windows 8.1 and Windows Server 2012 R2 May 2020 Security Update
HIGH	9.3	137262	KB4561673: Windows 8.1 and Windows Server 2012 R2 June 2020 Security Update
HIGH	9.3	138463	KB4565540: Windows 8.1 and Windows Server 2012 R2 July 2020 Security Update
HIGH	9.3	139489	KB4571723: Windows 8.1 and Windows Server 2012 R2 August 2020 Security Update

Рисунок 3.12 – Перелік та класифікація найбільш критичних виявлених вразливостей серверу Supermicro

3	17	30	2	124
CRITICAL	HIGH	MEDIUM	LOW	INFO

Severity	CVSS v2.0	Plugin	Name
CRITICAL	10.0	142686	KB4586823: Windows 8.1 and Windows Server 2012 R2 November 2020 Security Update
CRITICAL	10.0	147229	KB5000853: Windows 8.1 and Windows Server 2012 R2 March 2021 Security Update
CRITICAL	10.0	148477	KB5001382: Windows 8.1/RT and Windows Server 2012 R2 Apr 2021 Security Update
HIGH	9.3	91230	7-Zip < 16.00 Multiple Vulnerabilities
HIGH	9.3	137262	KB4561673: Windows 8.1 and Windows Server 2012 R2 June 2020 Security Update
HIGH	9.3	138463	KB4565540: Windows 8.1 and Windows Server 2012 R2 July 2020 Security Update
HIGH	9.3	139489	KB4571723: Windows 8.1 and Windows Server 2012 R2 August 2020 Security Update

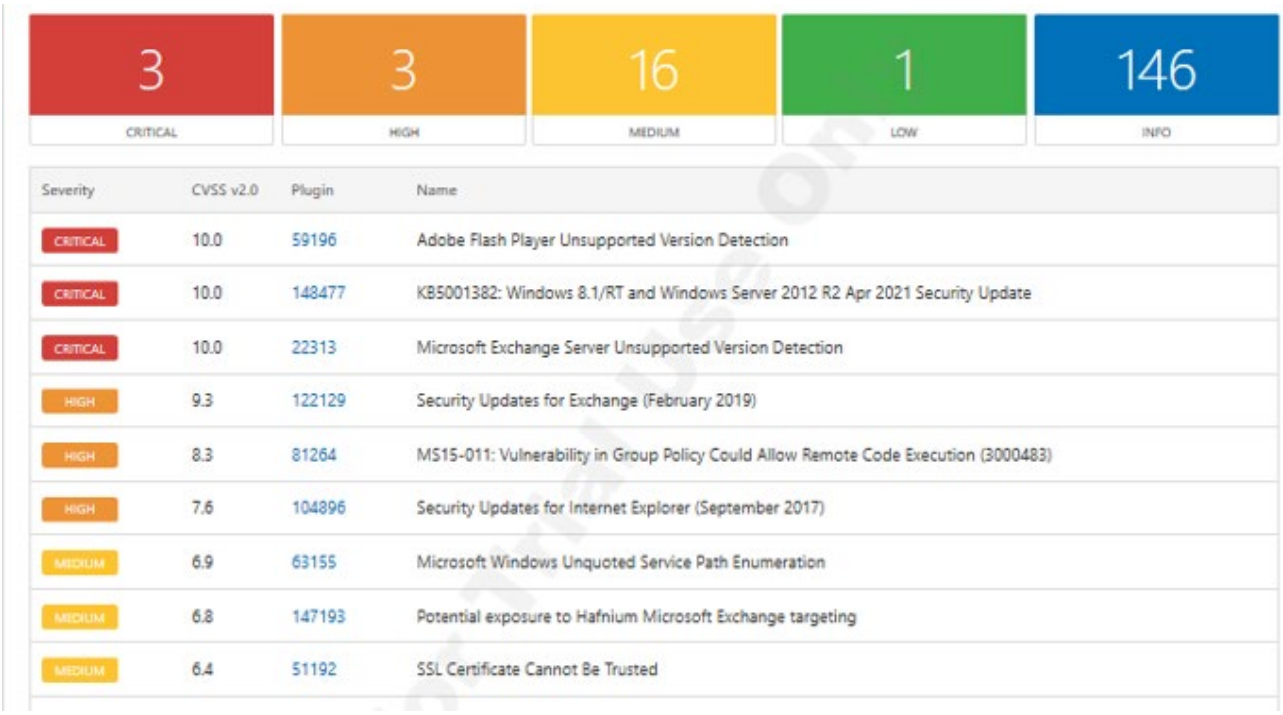
Рисунок 3.13 – Перелік та класифікація найбільш критичних виявлених вразливостей серверу HP ProLiant ML350

В результаті проведення автоматизованого сканування на вразливості основних віртуальних серверів, які організовані на сервері віртуалізації Supermicro, отримані слідуючі результати.

3	3	11	2	124
CRITICAL	HIGH	MEDIUM	LOW	INFO

Severity	CVSS v2.0	Plugin	Name
CRITICAL	10.0	147229	KB5000853: Windows 8.1 and Windows Server 2012 R2 March 2021 Security Update
CRITICAL	10.0	148477	KB5001382: Windows 8.1/RT and Windows Server 2012 R2 Apr 2021 Security Update
CRITICAL	10.0	101365	Windows 8.1 and Windows Server 2012 R2 July 2017 Security Updates
HIGH	8.3	81264	MS15-011: Vulnerability in Group Policy Could Allow Remote Code Execution (3000483)
HIGH	7.6	104896	Security Updates for Internet Explorer (September 2017)
HIGH	7.5	146341	KB4601349: Windows 8.1 and Windows Server 2012 R2 February 2021 Security Update
MEDIUM	6.4	51192	SSL Certificate Cannot Be Trusted
MEDIUM	6.4	57582	SSL Self-Signed Certificate
MEDIUM	6.1	104743	TLS Version 1.0 Protocol Detection

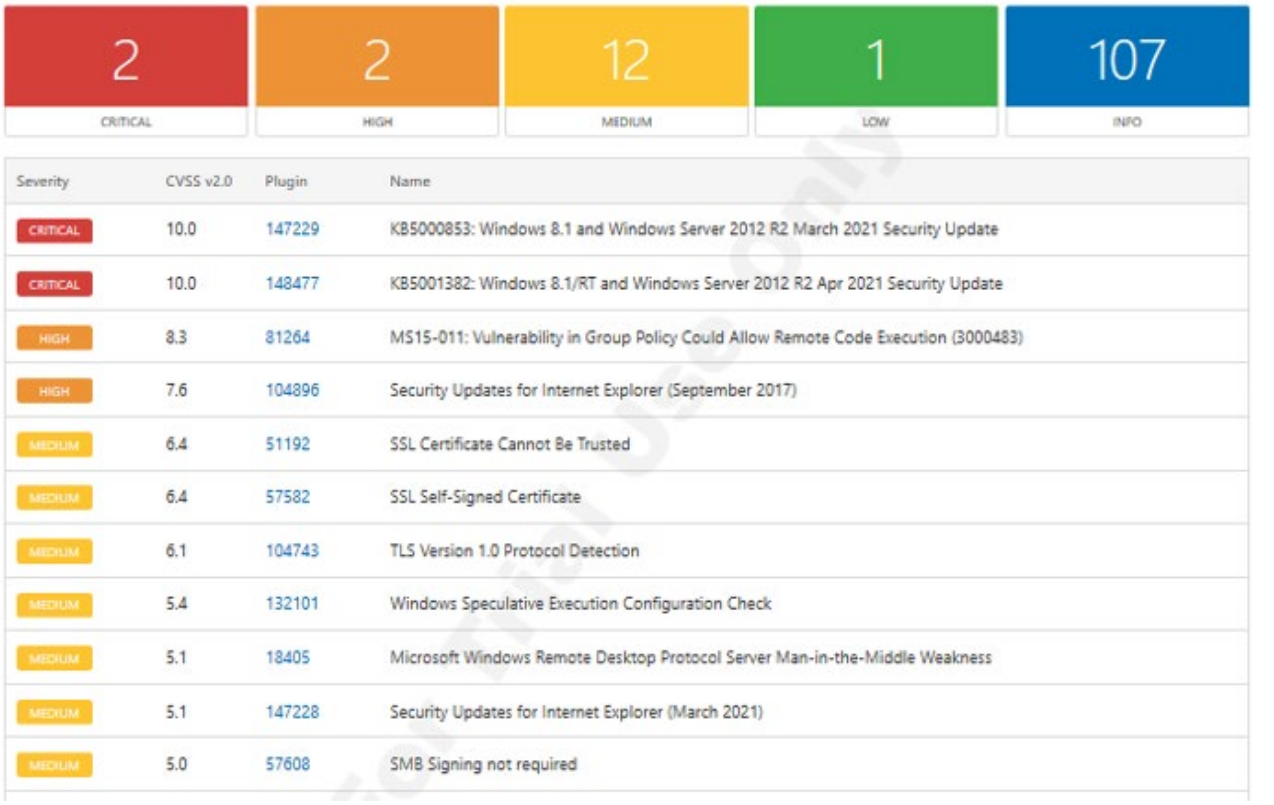
Рисунок 3.14 – Перелік та класифікація найбільш критичних виявлених вразливостей віртуального серверу DC-01



3	3	16	1	146
CRITICAL	HIGH	MEDIUM	LOW	INFO

Severity	CVSS v2.0	Plugin	Name
CRITICAL	10.0	59196	Adobe Flash Player Unsupported Version Detection
CRITICAL	10.0	148477	KB5001382: Windows 8.1/RT and Windows Server 2012 R2 Apr 2021 Security Update
CRITICAL	10.0	22313	Microsoft Exchange Server Unsupported Version Detection
HIGH	9.3	122129	Security Updates for Exchange (February 2019)
HIGH	8.3	81264	MS15-011: Vulnerability in Group Policy Could Allow Remote Code Execution (3000483)
HIGH	7.6	104896	Security Updates for Internet Explorer (September 2017)
MEDIUM	6.9	63155	Microsoft Windows Unquoted Service Path Enumeration
MEDIUM	6.8	147193	Potential exposure to Hafnium Microsoft Exchange targeting
MEDIUM	6.4	51192	SSL Certificate Cannot Be Trusted

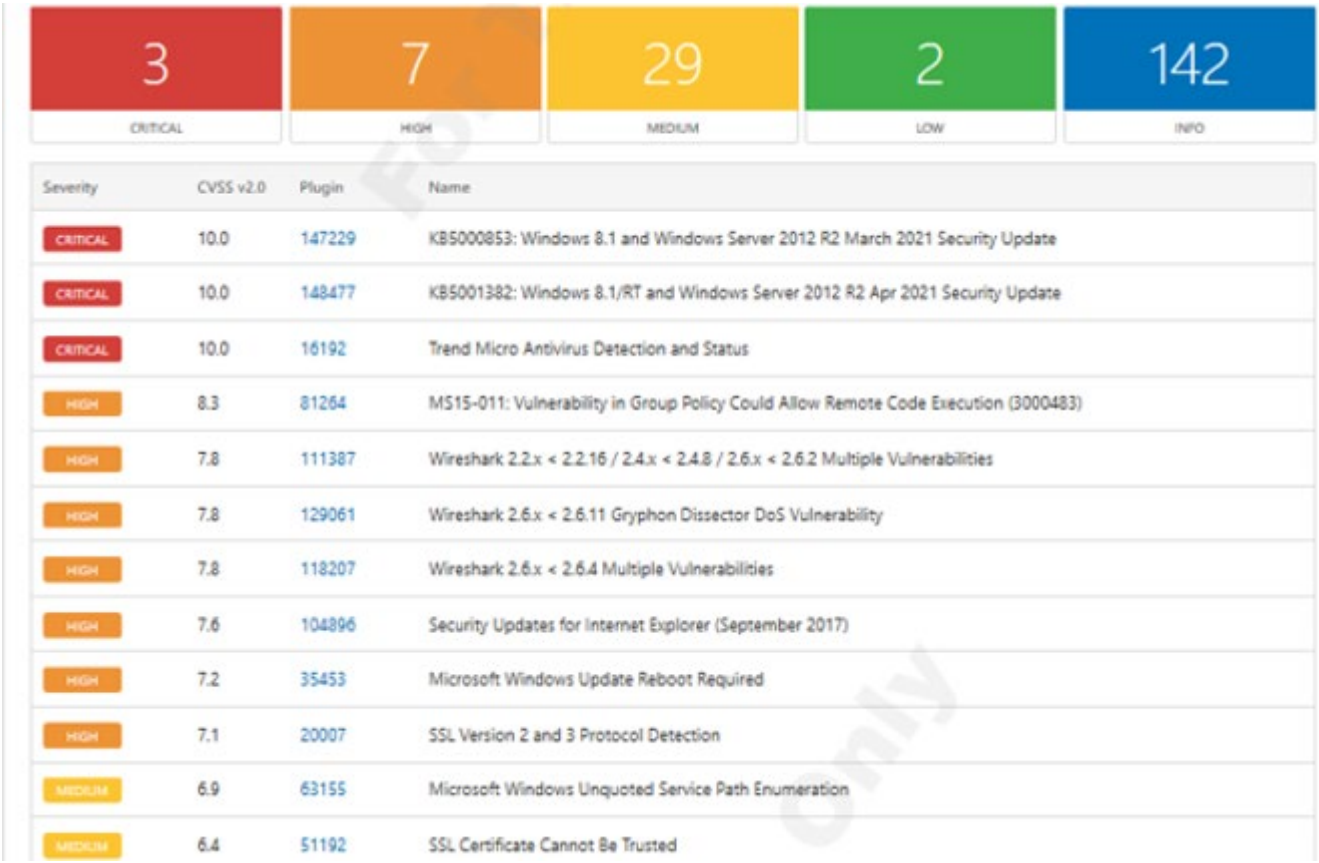
Рисунок 3.15 – Перелік та класифікація найбільш критичних виявлених вразливостей віртуального серверу Mail-01 Exchange2016



2	2	12	1	107
CRITICAL	HIGH	MEDIUM	LOW	INFO

Severity	CVSS v2.0	Plugin	Name
CRITICAL	10.0	147229	KB5000853: Windows 8.1 and Windows Server 2012 R2 March 2021 Security Update
CRITICAL	10.0	148477	KB5001382: Windows 8.1/RT and Windows Server 2012 R2 Apr 2021 Security Update
HIGH	8.3	81264	MS15-011: Vulnerability in Group Policy Could Allow Remote Code Execution (3000483)
HIGH	7.6	104896	Security Updates for Internet Explorer (September 2017)
MEDIUM	6.4	51192	SSL Certificate Cannot Be Trusted
MEDIUM	6.4	57582	SSL Self-Signed Certificate
MEDIUM	6.1	104743	TLS Version 1.0 Protocol Detection
MEDIUM	5.4	132101	Windows Speculative Execution Configuration Check
MEDIUM	5.1	18405	Microsoft Windows Remote Desktop Protocol Server Man-in-the-Middle Weakness
MEDIUM	5.1	147228	Security Updates for Internet Explorer (March 2021)
MEDIUM	5.0	57608	SMB Signing not required

Рисунок 3.16 – Перелік та класифікація найбільш критичних виявлених вразливостей віртуального серверу FS-01



3	7	29	2	142
CRITICAL	HIGH	MEDIUM	LOW	INFO

Severity	CVSS v2.0	Plugin	Name
CRITICAL	10.0	147229	KB5000853: Windows 8.1 and Windows Server 2012 R2 March 2021 Security Update
CRITICAL	10.0	148477	KB5001382: Windows 8.1/RT and Windows Server 2012 R2 Apr 2021 Security Update
CRITICAL	10.0	16192	Trend Micro Antivirus Detection and Status
HIGH	8.3	81264	MS15-011: Vulnerability in Group Policy Could Allow Remote Code Execution (3000483)
HIGH	7.8	111387	Wireshark 2.2.x < 2.2.16 / 2.4.x < 2.4.8 / 2.6.x < 2.6.2 Multiple Vulnerabilities
HIGH	7.8	129061	Wireshark 2.6.x < 2.6.11 Gryphon Dissector DoS Vulnerability
HIGH	7.8	118207	Wireshark 2.6.x < 2.6.4 Multiple Vulnerabilities
HIGH	7.6	104896	Security Updates for Internet Explorer (September 2017)
HIGH	7.2	35453	Microsoft Windows Update Reboot Required
HIGH	7.1	20007	SSL Version 2 and 3 Protocol Detection
MEDIUM	6.9	63155	Microsoft Windows Unquoted Service Path Enumeration
MEDIUM	6.4	51192	SSL Certificate Cannot Be Trusted

Рисунок 3.17 – Перелік та класифікація найбільш критичних виявлених вразливостей віртуального серверу UKRS02SQLV

На вказаних віртуальних серверах виявлені критичні вразливості, які за умови знаходження всередині мережі підприємства, можуть бути використані неавторизованим користувачем для доступу до даних, їх видалення, перехоплення паролів користувачів, зупинення та модифікації сервісів, програмного забезпечення.

В результаті перевірки застосовуваних політик Active Directory на серверах і робочих станціях було виявлено, що Active Directory має просту структуру - один ліс та один домен. Рівень лісу та домену 2012 R2. За данний сервіс відповідає один контроллер домену - dc01.local з усіма ролями та одним сайтом за замовчуванням. Проведено діагностику служб контролеру домена, в результаті якої усі тести пройдено, проблем не виявлено.

Нижче перераховано групові політики домену dc01.local та фактичний результат застосування групових політик на серверах.

Таблиця 3.2

Групові політики застосовані на комп’ютерах у домені

GPO	Домени, до яких підключено GPO	На яких комп’ютерах застосовується
Default Domain Controllers Policy	Domain Controllers	DC01
Default Domain Policy	Domain.local	Усі комп’ютери домену
Mount Disk S	Domain.local	Усі комп’ютери домену

Таблиця 3.3

Групові політики застосовані на віртуальних серверах у домені

Сервер	Застосовані групові політики (COMPUTER SETTINGS)	Застосовані групові політики (USER SETTINGS)
DC01	Default Domain Controllers Policy Default Domain Policy Local Group Policy	Default Domain Policy Mount Disk S
FS01	Default Domain Policy	Default Domain Policy Mount Disk S
MAIL01	Default Domain Policy Local Group Policy	Default Domain Policy Mount Disk S
Zabbix	Default Domain Policy Local Group Policy	Default Domain Policy Mount Disk S
Customs-SRV	Default Domain Policy	Default Domain Policy Mount Disk S
TS01	Default Domain Policy Local Group Policy	Default Domain Policy Mount Disk S
UKRS02SQLV	Default Domain Policy	Default Domain Policy Mount Disk S
VeeamOne	Default Domain Policy	Default Domain Policy Mount Disk S

Політика паролів:

- запам’ятовуються останні 24 паролі
- максимальний вік пароля — 42 дні
- мінімальний вік пароля — 1 день
- пароль повинен відповідати вимогам складності

В Active Directory три групові політики. Дві політики за замовчуванням та одна «Mount Disk S», створена для монтування мережевого диску.

При проведенні дослідження сервери та робочі станції було просканово антивірусним сканером Microsoft Safety Scanner. Нижче наведено результати та опис загроз, знайдених сканером. Більшість із них є програмами, що використовуються для активації неліцензованого ПЗ (здебільшого компанії Microsoft: Windows, Office).

Таблиця 3.4

Загрози та їх опис, виявлені сканером Microsoft Safety Scanner

Загроза	Назва серверу	Назва робочої станції	Категорія	Стислий опис загрози
Adware:Win32/ Hiru	—	VKOPC	Відображення реклами	Це програмне забезпечення здатне відображати рекламу, коли користувач переглядає веб-сторінки.
HackTool:MSIL/ AutoKms	—	WS33	Засоби для «зламування» програмного забезпечення	Найчастіше використовуються, щоб змусити ПЗ працювати без ліцензійного ключа. Є потенційно небезпечними, оскільки крім прямого призначення можуть виконувати шкідливі дії. Також із активаторами
HackTool:MSIL/ AutoKMS.I!MTB	Ukrs02SQLV	KROMKA02, KROMKA03, VKOPC, WS06, WS07, WS10, WS12,		

		WS13, WS15, WS17, WS24, WS27, WS28, WS31, WS33		може розповсюджуватись шкідливе ПЗ.
HackTool:Win32/AutoKMS	FS01, Ukrs02SQLV	KROMKA02, KROMKA03, VKOPC, WS01, WS02, WS04, WS05, WS06, WS07, WS08, WS09, WS10, WS12, WS13, WS14, WS15, WS17, WS19, WS22, WS23, WS24,		

		WS25, WS27, WS28, WS31, WS32, WS33		
HackTool:Win32/AutoKMS.NK!MTB	—	WS06, WS28		
HackTool:Win32/AutoKMS.S!MTB	—	VKOPC		
HackTool:Win32/KMSActivator.A!MSR	—	WS06, WS07		
HackTool:Win32/WinActivator	VM-Client1	—		
HackTool:Win32/ActivateRadmin	FS01	VKOPC, WS04		
HackTool:Win32/RemoteAdmin	FS01	—		
HackTool:Win32/Keygen	FS01	VKOPC, WS04, WS10, WS13	Генерація ключів	Використовується для генерації ключів для неліцензованого ПЗ. Є потенційно небезпечним, оскільки із генераторами ключів може роз пов сюд жу ва тись шкідливе ПЗ.
HackTool:Win32/Keygen.A	FS01	VKOPC, WS07, WS13		

Trojan:Win32/CrypInject		VKOPC	Троянські програми	«Трояни» розповсюджуються під виглядом корисного ПЗ, але можуть виконувати на враженому комп'ютері різні шкідливі дії і надавати зловмисникам несанкціонований доступ до комп'ютера.
Trojan:Win32/Vigorf.A	FS01	—		
Trojan:Win32/Orsam!rfn	—	VKOPC		
VirTool:Win32/DefenderTamperingRestore	—	KROMKA02, KROMKA03, VKOPC, WS04, WS05, WS06, WS07, WS08, WS09, WS10, WS12, WS13, WS17, WS19, WS22, WS24, WS28, WS31, WS33	Зниження рівня захисту	Було виявлено налаштування Microsoft Defender, які відрізняються від оптимальних і можуть запобігати формальному функціонуванню Microsoft Defender і виявленню ним загроз.

Exploit:ASP/CVE-2021-27065	Mail01	—	Вразливість Exchange Server	Вразливість використовується при атаках «наземних» поштових серверів Exchange. Вразливість може бути використана для отримання доступу до облікових записів пошти користувачів, а також для встановлення на сервер шкідливого ПЗ, яке надає зловмиснику довгостроковий доступ до поштового сервера.
Trojan:Win32/Chadivendo.STE	Mail01	—	Троянські програми	«Трояни» можуть виконувати на враженому комп’ютері різні шкідливі дії і надавати зловмисникам несанкціонований доступ до комп’ютера.
Trojan:Win32/Chadivendo.STA	Mail01	—		
Trojan:Win32/Amynex.A	Mail01	—		
Trojan:Win32/Nanocore.VH!MSR	Mail01	—		
Trojan:PowerShell/LemonDuck.B	Mail01	—		Скрипт PowerShell, який може видаляти з системи антивірусні продукти і створювати задачі у

				планувальнику задач Windows.
Backdoor:ASP/Chopper.P!dha	Mail01	—	Отримання несанкціонованого доступу	Використовуються для надання зловмиснику доступу до вражених комп’ютерів.

Більшість виявлених антивірусом об’єктів є засобами для генерації ключів та активації неліцензованого ПЗ. Також виявлено декілька загроз, класифікованих як троянські програми. Деякі виявлені об’єкти класифіковано як потенційно небезпечні програми – рішення щодо їх використання залишається за адміністратором.

На поштовому сервері виявлено вразливість CVE-2021-27065, яка дає змогу отримати несанкціонований доступ до поштового сервера, а також багато шкідливих об’єктів серед файлів Exchange Server, у планувальнику задач Windows.

Проведена перевірка налаштувань роботи брандмауера FireWall. Нижче наведено статус брандмауера на серверах. З таблиці видно, що на більшості серверів вимкнено брандмауер для мереж, до яких ці сервери підключені.

Таблиця 3.5

Статус брандмауера на серверах

Сервер	Доменні мережі		Приватні мережі		Публічні мережі	
	Підключено	Брандмауер активовано	Підключено	Брандмауер активовано	Підключено	Брандмауер активовано
DC01		Ні		Ні	+	Ні
FS01	+	Ні		Ні		Так

MAIL01	+	Ні		Ні		Так
CUSTOMS-SRV		—		Ні	+	Ні
Zabbix		—		Ні	+	Так
TS01	+	Так		Так		Так
UKRS02SQLV	+	Ні		Так		Ні
VeeamOne	+	Ні		Ні		Ні

Сервер		DC01	FS01	MAIL01	CUSTOMS-SRV	Zabbix	TS01	UKRS02SQLV	VeeamOne
Доменні мережі	Підключено		Так	Так			Так	Так	Так
	Брендмауер активовано	Ні	Ні	Ні	—	—	Так	Ні	Ні
Приватні мережі	Підключено								
	Брендмауер активовано	Ні	Ні	Ні	Ні	Ні	Так	Так	Ні
Публічні мережі	Підключено	Так			Так	Так			
	Брендмауер активовано	Ні	Так	Так	Ні	Так	Так	Ні	Ні

Оцінка актуальності оновлень ОС та антивірусного ПЗ на серверах компанії наведені в таблиці нижче.

Таблиця 3.6

Оновлення антивірусного ПЗ та ОС на серверах

Сервер	Антивіруси	Оновлення ОС

DC01	ESET File Security (увімкнено, оновлено)	Дата останнього встановлення оновлень: 16.01.2022 Доступні оновлення: KB4603004 2021-02 Security and Quality Rollup for .NET Framework 3.5, 4.5.2, 4.6, 4.6.1, 4.6.2, 4.7, 4.7.1, 4.7.2, 4.8 for Windows Server 2012 R2 for x64 KB5001382 2020-04 Security Monthly Quality Rollup for Windows Server 2012 R2 for x64-based Systems KB890830 Windows Malicious Software Removal Tool x64 - v5.88
FS01	ESET File Security (увімкнено не всі компоненти, оновлено, програма вимагає перезавантажити комп’ютер)	Дата останнього встановлення оновлень: 16.02.2022 Доступні оновлення: KB5001382 2023-04 Security Monthly Quality Rollup for Windows Server 2012 R2 for x64-based Systems KB890830 Windows Malicious Software Removal Tool x64 - v5.88
MAIL01	Антивірус не встановлено	Дата останнього встановлення оновлень: 12.04.2021 Доступні оновлення: KB5001382

		2021-04 Security Monthly Quality Rollup for Windows Server 2012 R2 for x64-based Systems KB890830 Windows Malicious Software Removal Tool x64 - v5.88 KB4577586 Update for Removal of Adobe Flash Player for Windows Server 2012 R2 for x64-based systems
CUSTOMS-SRV	Антивірус не встановлено	Дата останнього встановлення оновлень: 16.04.2022 Доступні оновлення: KB4535680 2021-01 Security Update for Windows Server 2012 R2 for x64-based Systems KB4603004 2021-02 Security and Quality Rollup for .NET Framework 3.5, 4.5.2, 4.6, 4.6.1, 4.6.2, 4.7, 4.7.1, 4.7.2, 4.8 for Windows Server 2012 R2 for x64
Zabbix	Антивірус не встановлено	Дата останнього встановлення оновлень: 22.01.2024 Доступних оновлень немає.
TS01	Антивірус не встановлено	Дата останнього встановлення оновлень: 16.04.2023 Доступних оновлень немає.

UKRS02SQLV	Trend Micro Worry-Free Business Security Agent (увімкнено, оновлено)	Дата останнього встановлення оновлень: 16.01.2022 Необхідно перезавантажити комп'ютер для завершення встановлення оновлень та перевірки наявності доступних оновлень.
VeeamOne	Антивірус не встановлено	Дата останнього встановлення оновлень: 06.09.2020 Не вдалося перевірити наявність оновлень — помилка 8024402C.

З таблиці видно, що на більшості серверів необхідно встановити важливі оновлення ОС, відсутнє антивірусне програмне забезпечення.

Аналіз серверної інфраструктури в розрізі надійності та безпеки показав, що в цілому, серверна інфраструктура не є достатньо надійною, слід звернути особливу увагу на наступні аспекти:

1. Застарілі фізичні сервери (2012-2013 року випуску) мають потенційний ризик вийти з ладу;
2. Організація системи віртуалізації з роллю Hyper-V на одному фізичному сервері не є відмовостійким рішенням, тому у разі його зупинки може спричинити відмову усіх сервісів в організації;
3. Сервер резервного копіювання не має додаткової точки збереження резервних копій (відсутній холодний резерв);
4. Не налаштовані сповіщення у системі моніторингу VeeamOne і в завданнях серверу резервних копій Veeeam B&R, що збільшує час на виявлення і своєчасне реагування на проблеми на фізичному та віртуальних серверах та системі резервного копіювання даних;
5. Операційна система для фізичних і віртуальних серверів – Windows 2012 R2. У 2023 році для цієї ОС припинилася офіційна підтримка Microsoft;

6. Не на всіх серверах встановлені актуальні оновлення ОС та безпеки;

7. На більшості серверів відсутнє антивірусне ПО;

8. На більшості серверів брандмауер вимкнено для мереж, до яких ці сервери підключені;

9. Виявлені критичні вразливості, які за умови знаходження неавторизованого користувача всередині мережі, можуть бути використані для доступу до даних, їх видалення, перехоплення паролів користувачів;

10. На поштовому сервері виявлено вразливість CVE-2021-27065, яка дає змогу отримати несанкціонований доступ до поштового сервера;

11. Сервіс Active Directory не має резервного контролеру домену. В разі виходу з ладу єдиного контролеру домену, виникне проблема авторизації в системі, що призведе до простою робочого процесу на час відновлення контролеру AD з резервної копії;

12. Сервіс DHCP не має відмовостійкості (Failover DHCP), в разі відмови сервісу – клієнтии (пристрої) не зможуть отримувати ip адресу, тим самим не будуть мати доступ до локальної та глобальної мереж;

13. Ввімкнений вбудований доменний та локальний обліковий запис Administrator, що може спростити підбір пароля зловмисником за рахунок відомого логіну.

3.3 Тестування на проникнення

В межах даного розділу проведено перевірку стійкості зовнішнього периметру мережі до атак та проникнення. За допомогою спеціалізованих інструментів для тестування на проникнення спроби встановити зовнішнє підключення до мережі та проникнути у внутрішню мережу ззовні виявилися невдалими. З метою забезпечення конфіденційності деякі наведені на рисунках в цьому розділі IP адреси та доменні імена приховані.

Під час проведення тестування на проникнення було використано набір програмного забезпечення, що входить в комлект з операційною системою Kali Linux, а саме:

Dnsmap. Оскільки за допомогою сайту підприємства приблизно відомо патерн домену підприємства, використовується дана утиліта для пошуку пов’язаних доменів та адрес, за якими вони знаходяться. Таким чином ми отримуємо адресу, що буде використано для подальшого проникнення.

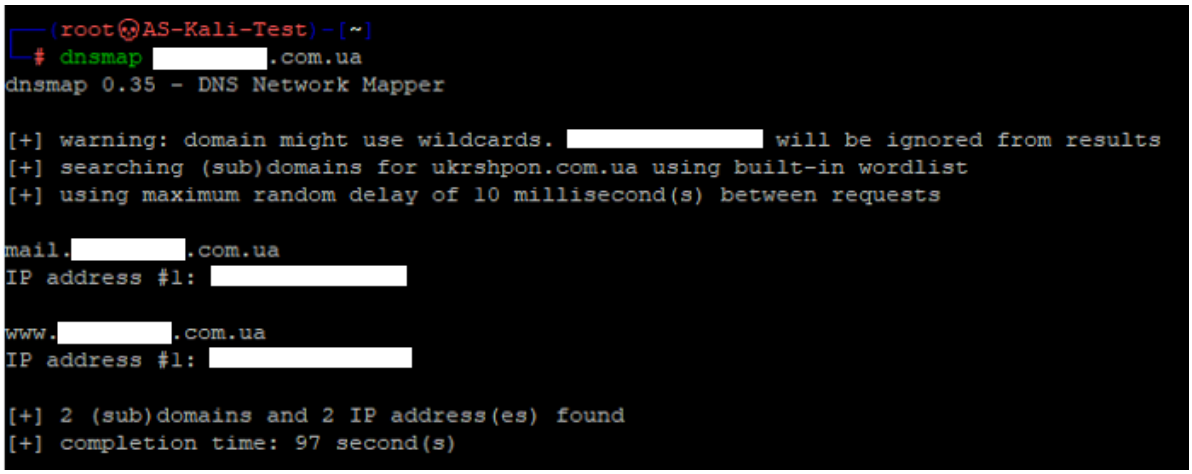


Рисунок 3.18 - Пошук пов’язаних доменів за патерном

Nmap. В результаті сканування виявлено, що маршрутизатор-файервол Sophos gateway, в тому числі, блокує сканування портів/сервісів, окрім необхідних для роботи сайту та поштового сервісу, через які не вдалося виконати зовнішнє вторгнення суто технічними засобами. Спроба сканування SMTP-користувачів також виявилась невдалою.

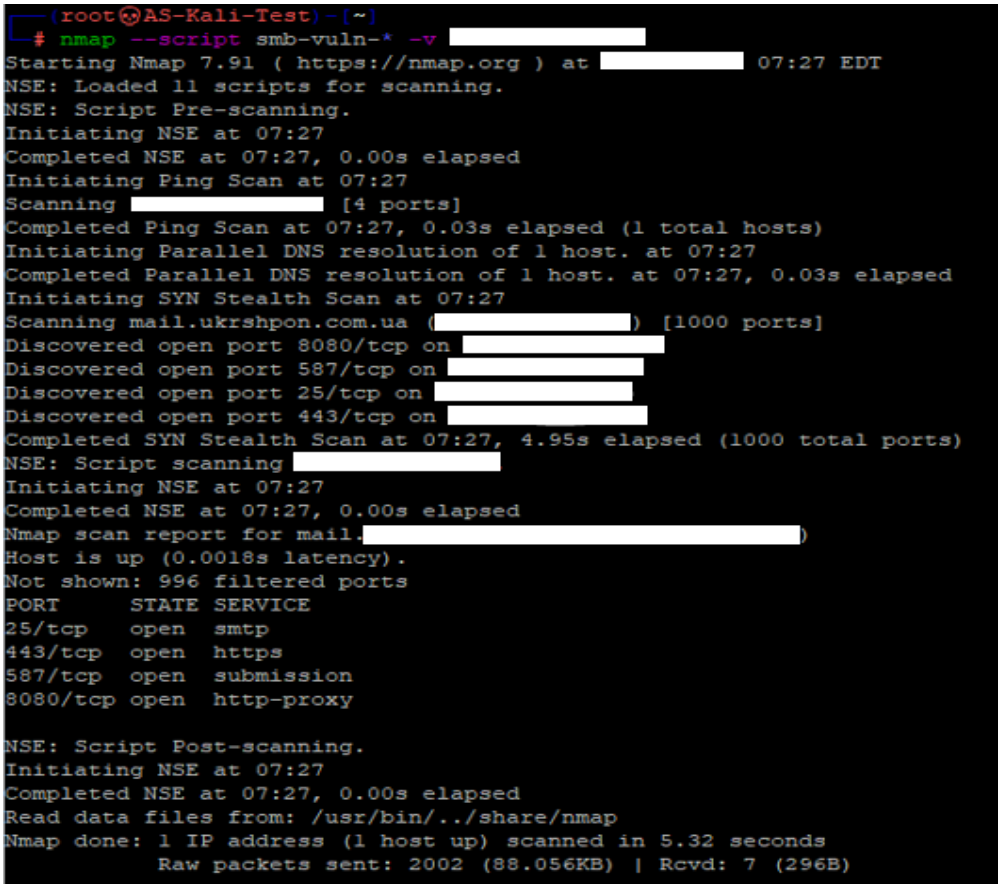


Рисунок 3.19 - Пошук відкритих портів на маршрутизаторі-файерволі

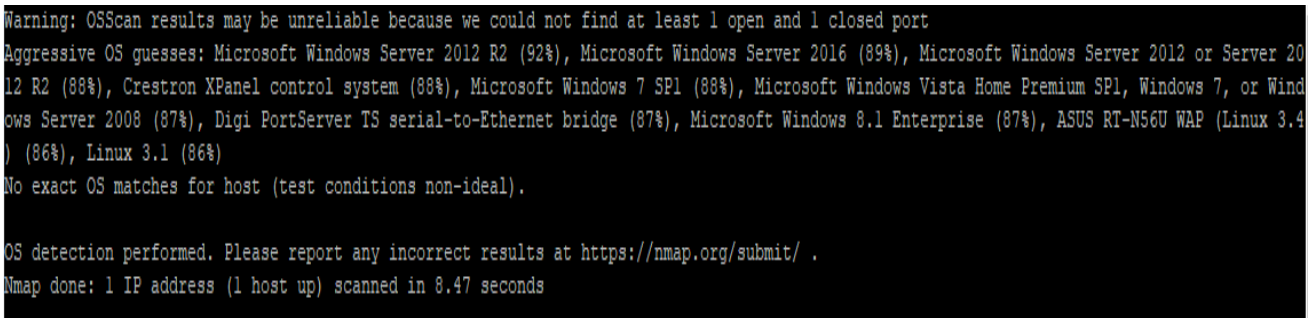


Рисунок 3.20 - Виявлення операційної системи за визначеною адресою

Рисунок 3.21 – Невдала спроба отримати перелік користувачів поштової системи

Metasploit. Дане програмне забезпечення використовується для спроби експлуатації виявлених загроз. Оскільки основна частина сервісів недоступні для сканування ззовні, спробуємо використати лише декілька базових експлоїтів - операційної системи сервера, протоколу SMTP, а також веб-консолі Outlook.

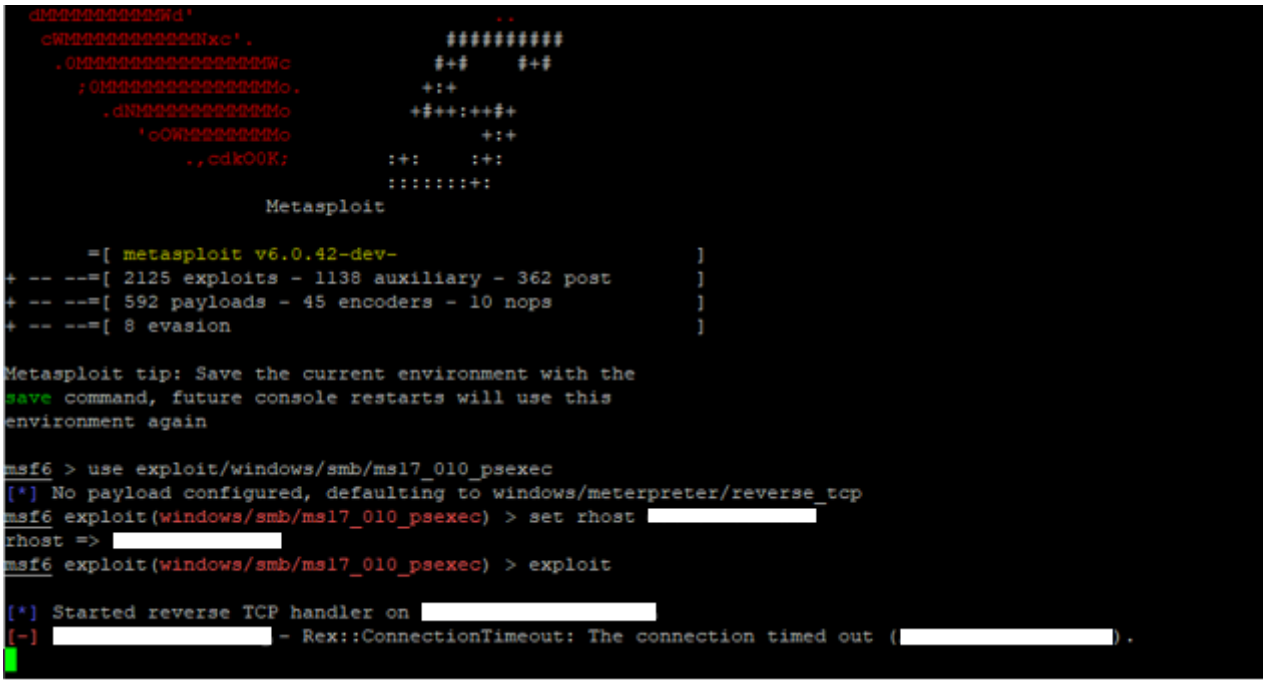


Рисунок 3.22– Невдала спроба експлуатації вразливості в операційній системі

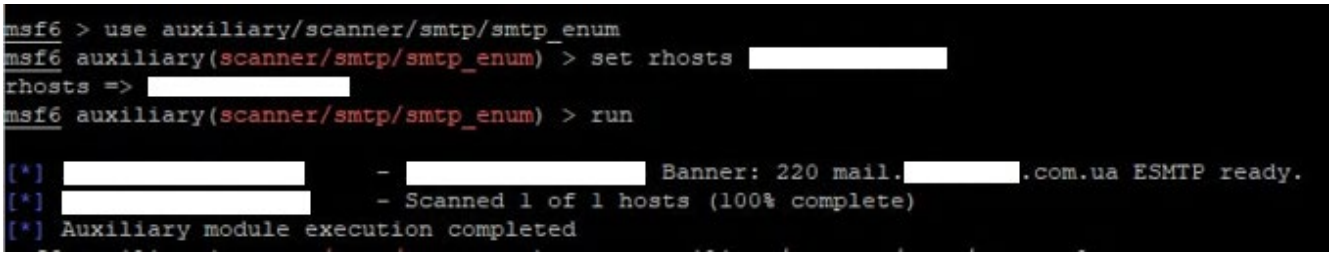


Рисунок 3.23 – Невдала спроба експлуатації вразливості в SMTP-протоколі для отримання даних поштових сервісів

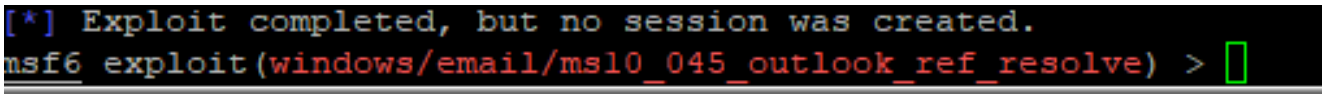


Рисунок 3.24 - Невдала спроба експлуатації вразливості в веб-інтерфейсі Outlook

Можна констатувати, що спроба використання вищевказаних експлоітів виявилась невдалою. Також вивлено, що окремих робочих станціях у користувачів залишилися права локального адміністратора, що є джерелом додатковим загрози.

Проводимо перевірку стійкості веб-сайту до атак, намагаємось зупинити роботу ресурсу або підмінити тестову сторінку. Сайт підприємства використовує nginx у якості веб-сервера, Joomla в якості CMS і має IP-адресу. Сам сайт знаходиться на хостинг-майданчику і не має прямого зв'язку з корпоративною мережею.

Сканування на вразливості проводимо інструментами OWASP ZAP і Joomscan.

За результатами сканування інструментом OWASP ZAP було виявлено декілька вразливостей:

ZAP Scanning Report

Summary of Alerts

Risk Level	Number of Alerts
High	2
Medium	2
Low	5
Informational	2

Alerts

Name	Risk Level	Number of Instances
Cross Site Scripting (Reflected)	High	1
SQL Injection	High	1
Vulnerable JS Library	Medium	1
X-Frame-Options Header Not Set	Medium	249
Absence of Anti-CSRF Tokens	Low	9
Cookie No HttpOnly Flag	Low	386
Cookie Without SameSite Attribute	Low	386
Cross-Domain JavaScript Source File Inclusion	Low	211
X-Content-Type-Options Header Missing	Low	472
Information Disclosure - Suspicious Comments	Informational	17
Timestamp Disclosure - Unix	Informational	92

Рисунок 3.25 – Перелік та класифікація вразливостей веб-ресурсу

Вразливості за рейтингом ризику «High» вказані в переліку нижче:

1) Cross Site Scripting (Reflected) – вразливість, що потенційно дозволяє зловмиснику виконати код на комп’ютері користувача сайту. Тим не менш, для її виконання на сайті, зловмиснику необхідно самостійно сконструювати посилання і змусити користувача на нього перейти.

2) SQL Injection – потенційно, на сайті можливе виконання SQL-ін’єкції.

Для захисту від зазначених вразливостей, рекомендується регулярно оновлювати програмне забезпечення веб-сайту та CMS, а також екранувати всі дані, що користувач вводить на сайті, задля того, щоб унеможливити виконання стороннього коду.

Також, за допомогою інструмента Joomscan, було просканована CMS Joomla, яка використовується на сайті. Було виявлено версію Joomla 2.5.19 і наступні потенційні вразливості:

Таблиця 3.7

Потенційні вразливості веб-сайту

Назва вразливості	CVE
Joomla! Core Remote Privilege Escalation Vulnerability	CVE-2016-9838
Joomla! Component Akeeba Kickstart - Unserialize Remote Code Execution	CVE-2014-7228
Joomla! Core Authentication Bypass Vulnerability	CVE-2014-6632
Joomla HTTP Header Unauthenticated Remote Code Execution	CVE-2015-8562
PHPMailer Remote Code Execution Vulnerability	CVE-2016-10033
PPHPMailer Incomplete Fix Remote Code Execution Vulnerability	CVE-2016-10045

Було виконано спроби експлатувати знайдені вразливості, але вони виявились невдалими:

Таблиця 3.8

Результати спроб експлуатації знайдених вразливостей веб-сайту

Назва вразливості	Хід експлуатації
Joomla! Core Remote Privilege Escalation Vulnerability	Дана вразливість може бути експлуатована лине в 3.X версіях CMS Joomla.

Joomla! Component Akeeba Kickstart - Unserialize Remote Code Execution	Дана вразливість може бути експлуатована лише під час оновлення CMS Joomla.
Joomla! Core Authentication Bypass Vulnerability	Дана вразливість може бути експлуатована, лише якщо використовується LDAP-аутентифікація.
Joomla HTTP Header Unauthenticated Remote Code Execution	Хоча сама версія CMS Joomla э вразливою, для успішної експлуатації даної вразливості, необхідно, щоб на сайті також використовувалася вразлива версія PHP (5.4.45<, 5.5.29<, 5.6.13<). На сайті використовується більш нова версія PHP, що не дозволяє експлуатацію даної вразливості.
PHPMailer Remote Code Execution Vulnerability	Даний компонент не використовується в CMS.
PPHPMailer Incomplete Fix Remote Code Execution Vulnerability	Даний компонент не використовується в CMS.

Таким чином, під час проведення тесту на проникнення, не вдалося здійснити проникнення на сайт або підміну інформації на сторінці. Хоча, деякі компоненти сайту потребують оновлення, загалом, сайт можна вважати захищеним.

3.4 Обстеження, аналіз та виявлення вразливостей поштової системи

Поштова система організації організована на базі продукту Microsoft Exchange 2016, також використовується проксі для SMTP на шлюзі Sophos SG135

для попередньої фільтрації вхідних повідомлень електронної пошти. На момент проведення обстеження існує 58 поштових скриньок і одна поштова група.

Поштовий сервер - віртуальна машина з операційною системою Windows Server 2012R2 стандарт і встановленим програмним забезпеченням Microsoft Exchange 2016 cu10. На момент обстеження випущено оновлення Exchnage CU20. Встановлення оновлення операційної систем поштового сервера було проведено 12/04/2021.

При дослідженні існуючих параметрів захисту від шкідливого ПЗ на Sophos SG135 виявлено, що увімкнено сканування вхідних повідомлень під час передачі. Сканування відбувається під час транзакції поштового повідомлення та у разі виявлення шкідливого пз виконується відбивання листа. Сканування шкідливого пз встановлено в режим “Подвійне сканування” - виконується перевірка двома різними модулями сканування для підвищення захисту (це зменшує швидкість обробки листів). Задіяна фільтрація з поширеними типами файлів.

При дослідженні існуючих параметрів захисту від спаму на Sophos SG135 виявлено, що працює функція відбивання листа на етапі транзакції, ящо лист розцінено як підтвердженний спам. Задіяні чорні списки поштових серверів в реальному часі. Активовано відбивання листів, якщо сервер-відправник використовує недопустиме представлення HELO в заголовку протокола SMTP. Використовуються сірі списки для формування бази серверів-відправників - данний функціонал відбиває перший лист та додає відправника до тимчасової бази. Після повторної спроби відправки листа відправником - лист приймається. Працює функція BATV (перевірка тегу повернення) - дозволяє захиститись від підробки звітів про недоставку. Виконується перевірка записку SPF. Реагування спам-фільтру на спам та підвердженний спам - переміщення до карантину. Фільтр виразів та чорний список відправників не заповнений. У якості адреси “postmaster” вказана зовнішня адреса sherold@business-group.de. Поштова система ззовні має багаторівневу перевірку, що забезпечує гарний захист поштової системи та інфраструктури вцілому.

При дослідженні серверу поштових скриньок Exchange Mailbox виявлено, що на поштовому сервері Exchange задіяні всі транспортні агенти.

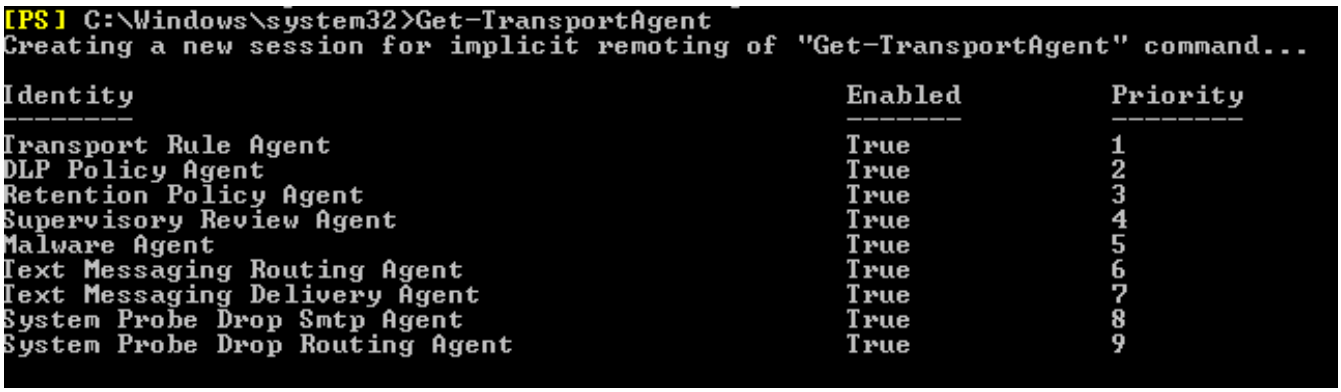


Рисунок 3.26 – Транспортні агенти на поштовому сервері Exchange

Фільтри поштового серверу увімкнені, але налаштування фільтрів відсутні. Доданих до списку блокувать або дозволів IP адрес, доменів, субдоменів та віправників немає. У разі виявлення підробного домену дій лист не переміщується до карантину або не відбивається. Поштова скринька карантину не задана. Параметри граничних значень (SCL) для видалення та переміщення задані як 9 - найвищий поріг небажанної пошти, але в параметрах задано, що при класифікації небажаних поштових повідомлень видалення або переміщення в карантин виконуватись не буде. Фільтрація контенту не наповнена фразами, які дозволені або не дозволені. Перевірка на наявність отримувача листа в організації не виконується. Правила для обробки поштового потоку відсутні.

При перевірці захисту поштової системи при отриманні шкідливих листів виконали відправку звичайного текстового повідомлення для оцінки швидкості надходження. Повідомлення було доставлено в поштову скриньку адміністратора приблизно через дві секунди після відправки. Виконали відправку повідомлення з вкладенням .txt у якому розташували два URL посилання. Лист не містив шкідливих посилань, але був перевірений та доставлений через 15 (пятнадцять) хвилин в поштову скринку адміністратора. Поштовий SMTP шлюз реагує на відправку тестового шкідливого коду та відхиляє повідомлення з відповідним

сповіщенням у випадку з Eicar в середині .txt файлу та у випадку, якщо .txt файл знаходиться в архіві (без пароля), а також виконує перевірку посилань. Потенційно шкідливі листи відфільтровуються ще до передачі листа від шлюза на поштовий сервер MS Exchange.

При перевірці логування подій на поштовому сервері подій, які можуть значно впливати на функціонування серверу – не знайдено. Але є події на які варто звернути увагу:

– На сервері встановлено агент SCOM, який не може приєднатися до серверу SCOM;

– Сертифікат аутентифікаці для федерації не знайдено;

– Робоча станція WS07 підключається до поштового сервера з неправильним логіном або паролем.

При аналізі поштової системи також виявлено, що адміністративна панель поштового серверу Exchange 2016 доступна з світу. Використовується стандартний адміністративний обліковий запис “Administrator” з правами адміністратора домена та поштового серверу, а також політика паролів Active Directory за замовчуванням. Всередині організації не має можливості виконати неавторизовану відправку листів на зовнішні домени.

В рамках анонсу від Microsoft з виявлення вразливості в Exchange проведено перевірку системи скриптом ProxyLogon.ps1:

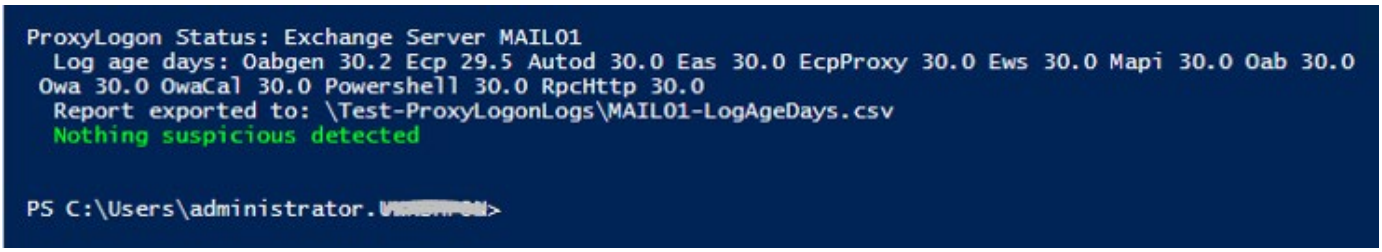


Рисунок 3.27 - Результат перевірки скриптом ProxyLogon

Згідно з результату роботи скрипта - поштовий сервер організації не було скомпрометовано, але за допомогою Microsoft Safety Scanner було виявлено

вразливість CVE-2021-27065, яка дає змогу отримати несанкціонований доступ до поштового сервера.

3.5 Розробка рекомендацій щодо усунення виявлених недоліків і вразливостей основних компонентів IT інфраструктури

В результаті виявлення вразливостей в мережевій інфраструктурі підприємства, розроблено слідуючі рекомендації з оптимізації мережевої інфраструктури:

1. Рекомендовано сформувати відмовостійке ядро мережі на основі двох комутаторів.
2. Рекомендовано підключити додаткового інтернет провайдера.
3. Рекомендовано сформувати відмовостійкий периметр мережі на основі двох маршрутизаторів-файерволів.
4. Рекомендовано налаштувати сервер збору файлів журналів (лог-сервер) і налаштувати обладнання для автоматичної відправки на нього файлів журналів.
5. Рекомендовано оновити програмне забезпечення мережевого обладнання до останньої можливої версії.
6. Рекомендовано розділити користувачів і сервери на дві різні логічні мережі (VLAN).
7. Рекомендовано зконфігурувати балансування навантаження на точках доступу Ubiquiti.
8. Рекомендовано провести радіопланування і визначити оптимальну кількість та розташування точок доступу для безперебійної роботи бездротової мережі.
9. Рекомендовано замінити D-Link на Ubiquiti.
10. Рекомендовано замінити комутатор SF-200 в центрі комутації №1 на більш сучасний і функціональний комутатор.
11. Рекомендовано налаштувати безпеку DHCP на комутаторах.

12. Рекомендовано налаштувати функціонал L2-безпеки на мережевому обладнанні.

13. Рекомендовано налаштувати функціонал 802.1X на комутаторах

При виявленні та дослідженні вразливостей в серверної інфраструктури та робочих станцій підприємства, розроблено слідуючі рекомендації з оптимізації:

1. Рекомендовано закрити критичні вразливості, які виявлені в серверній інфраструктурі.

2. Рекомендовано регулярно відслідковувати та встановлювати в плановому порядку оновлення для ОС серверів.

3. Рекомендовано виконати активацію ОС Windows на серверах.

4. Рекомендовано замінити фізичні сервери Supermicro (X9DRL-3F/iF) та HP ProLiant ML350 G5, зважаючи на термін їх експлуатації (сервери виробництва 2012-2013 року) на сучасні моделі та розглянути можливість організаціїї відмовостійкого рішення на базі Failover Hyper-v, розглянути можливість використання хмарних сервісів.

5. Рекомендовано додати другий контроллер домену в інфраструктуру для підвищення відмовостійкості сервісу AD.

6. Рекомендовано створити додатковий сервер DHCP та організувати FailOver DHCP.

7. Рекомендовано розглянути можливість переходу парку серверів з Windows Server 2012 r2 на нову операційну систему Windows Server 2019/2022, оскільки життєвий цикл ОС Windows Server 2012 r2 закінчився 2023 року.

8. Рекомендовано встановити антивірусне ПО на серверах у разі відсутності. Увімкнути брандмауер та зробити виключення у правилах для роботи необхідних сервісів.

9. Рекомендовано створити нового користувача з правами адміністратора в Active Directory, Exchange та на локальних серверах. Вимкнути й не використовувати вбудованого адміністративного користувача в Active Directory і на локальних серверах.

Основною проблемою, виявленою при обстеженні робочих станцій, є використання застарілого апаратного та програмного забезпечення, що має такі негативні наслідки:

1. Зниження рівня інформаційної безпеки організації через відсутність підтримки розробником застарілого ПЗ.
2. Підвищений ризик виходу з ладу застарілих комп'ютерів.
3. Зниження продуктивності співробітників (необхідність очікувати на увімкнення, «реакцію» системи на дії користувача).
4. Низька зручність роботи співробітників, які працюють із застарілими комп'ютерами.

Більш детально проблеми, бажані варіанти їх вирішення та можливі труднощі перелічено нижче в таблиці 3.9:

Таблиця 3.9

Виявлені проблеми з робочими станціями та рекомендації щодо їх усунення

№	Проблема	Назва робочої станції	Наслідки проблеми	Бажане вирішення	На що звернути увагу при вирішенні проблеми
1	Використання застарілої ОС (Windows 7)	14 робочих станцій: KROMKA01, WS01, WS02, WS11, WS14, WS15, WS16, WS18, WS20, WS21, WS25, WS26, WS27, WS32	1. ОС не підтримується компанією-розробником і не отримує оновлення безпеки — зниження рівня інформаційної безпеки.	Оновлення ОС до Windows 10	1. Сумісність програмного та апаратного забезпечення з новою ОС. 2. Невідповідність апаратних характеристик

			2. Низька зручність роботи співробітників, які працюють із застарілим ПЗ.		старих комп’ютерів вимогам нової ОС — необхідність модернізувати/замінити комп’ютер.
2	Застаріле апаратне забезпечення	Комп’ютери з процесорами старішими 2012 р. (яким є більше 10 років): KROMKA01, KROMKA02, KROMKA03, VKOPC, WS01, WS02, WS05, WS11, WS14, WS15, WS16, WS20, WS25, WS32	1. Підвищений ризик виходу з ладу застарілих комп’ютерів. 2. Зниження продуктивності та низька зручність роботи співробітників.	Заміна застарілих комп’ютерів на нові	Сумісність нового програмного та апаратного забезпечення з наявним
3	Система встановлена на HDD (не на SSD)	KROMKA01, KROMKA02, KROMKA03, WS01, WS02, WS05, WS09, WS11, WS14, WS16, WS17,	1. Повільна робота комп’ютерів. 2. Зниження продуктивності та низька зручність	Заміна HDD на SSD	Сумісність нового апаратного забезпечення з наявним.

		WS18, WS21, WS25, WS32	роботи співробітників.		

На кількох комп'ютерах знайдені загрози, класифіковані антивірусом як троянські програми - необхідно видалити ці загрози.

Після проведеного аналізу виявлених вразливостей поштової системи розроблено слідуючі рекомендації:

1. Рекомендовано виконати оновлення поштової системи - Exchange 2016 cu20, перевірити наявність вразливості CVE-2021-27065, встановити останні оновлення безпеки, виконати оновлення операційної системи поштового серверу.
2. Рекомендовано відключити доступ до адміністративної панелі керування з Інтернет.
3. Рекомендовано відредагувати політику формування адрес - прибрати домени, які не обслуговуються поштовим сервером.
4. Рекомендовано провести міграцію поштової системи на останню актуальну версію - Microsoft Exchange 2019.

Після дослідження проблем в роботі та вразливостей системи моніторингу розроблено слідуючі рекомендації:

1. Рекомендовано доналаштувати сервер моніторингу Zabbix і додати все необхідне обладнання, налаштувати сповіщення у випадку недоступності обладнання або перевищення порогових значень навантаження. Це дозволить максимально оперативно реагувати на події в корпоративній мережі.
2. Рекомендовано налаштувати сповіщення в системі моніторингу VeeamOne.
3. Рекомендовано заблокувати стандартний обліковий запис адміністратора або замінити стандартний пароль доступу.
4. Рекомендовано оновити Zabbix та VeeamOne до останньої можливої версії.

Після аудиту роботи системи резервного копіювання та відновлення розроблено слідуючі рекомендації:

1. Рекомендовано виконати оновлення ПЗ VeeamB&R та ОС Windows.
2. Рекомендовано організувати простір для холодного резерву файлів резервного копіювання.

3.6 Висновки до третього розділу

В результаті підготовки третього розділу роботи проведено практичне застосування набору інструментів та комплексу дій по виявленню вразливостей основних компонентів IT інфраструктури, реалізовано проект аудиту кібербезпеки, розроблені рекомендації з підвищення рівня кібехзахисту для типової компанії SMB сегменту. Поєднання організаційних та технічних методів з виявлення та усунення виявлених недоліків і вразливостей основних компонентів IT інфраструктури допоможуть суттєво підвищити рівень інформаційної безпеки та максимально захистити бізнес даної компанії.

ВИСНОВКИ

В результаті підготовки та написання роботи встановлено, що в сучасному світі половина кібератак направлена на малий та середній бізнес. IT інфраструктуру та дані SMB компаній, як правило, легше зламати та вкрасти. Малі та середні підприємства розуміють, що кіберзахист – це важливо, але досить часто не бажають вкладати кошти в його розвиток, хибно вважають, що інструменти кібербезпеки вже влаштовані в апаратне та програмне забезпечення, не підвищують кібергігієну та кіберкультуру своїх співробітників, не розуміють важливості системності цього процесу. Також велика кількість SMB підприємств не мають необхідної кількості та кваліфікації ресурсів для захисту від кіберзагроз та не розуміють за допомогою яких інструментів та комплексу дії вони можуть виявляти вразливості основних компонентів IT інфраструктури та підвищувати рівень кіберзахисту, забезпечувати необхідну безпеку своїх даних. Важливим моментом є розуміння та доступність організаційних та технічних механізмів, системне удосконалення та уніфікація програмно-апаратних засобів для виявлення вразливостей та підвищення рівня кібербезпеки основних компонентів IT інфраструктури компаній малого та середнього бізнесу. Маючи на озброєнні необхідні базові інструменти SMB сегмент може успішно протистояти викликам сьогодення в епоху Інтернету.

Кібербезпека - це складний, динамічний та постійний процес і він є важливим елементом успішності кожного бізнесу коли кожна компанія є цифровою і використовує в своїй діяльності новітні технології та сервіси .

В результаті написання першого розділу роботи встановлено причини недостанього рівня кіберзахисту, проблеми та їх наслідки, з якими зіштовуються SMB компанії, розкрито основні компоненти IT інфраструктури та важливість їх своєчасного та системного обслуговування. Загрози на основні компоненти та сервіси IT інфраструктури малих та середніх підприємств постійно зростають, змінюються, маневрують та завдають непоправної шкоди. Тому необхідно завжди

бути в курсі останніх кіберзагроз та найкращих практик, впроваджувати ефективні методи та засоби захисту.

В результаті написання другого розділу роботи розглянуті основні організаційні заходи по підвищенню рівня кіберзахисту на підприємствах малого та середнього сегменту, перелік базових тактик та технік аудиту кібербезпеки для основних компонентів IT інфраструктури.

Маючи набір інструментів та комплекс дій по виявленню вразливостей основних компонентів IT інфраструктури у SMB компаній є можливість вчасно виявляти вразливості та намагатися керувати ними, таким чином підвищуючи кіберзахист та збереження даних.

В результаті написання третього розділу роботи, на основі реалізації проекту з аудиту кібербезпеки, проведено практичне застосування набору інструментів та комплексу дій з виявлення вразливостей основних компонентів IT інфраструктури та тестування на проникнення зовнішнього периметру мережі, розроблені рекомендації щодо усунення виявлених недоліків та вразливостей, підвищення рівня кіберзахисту типової компанії малого та середнього бізнесу.

В результаті підготовки та написання роботи було виконано наступні задачі:

1. Розглянуто проблематику та аналіз кіберзагроз IT інфраструктури малих та середніх підприємств.
2. Розглянуто методи та засоби підвищення рівня кіберзахисту основних компонентів IT інфраструктури.
3. Запропоновано організаційні та технічні механізми з підвищення рівня кіберзахисту, розроблено рекомендації щодо усунення виявлених недоліків і вразливостей основних компонентів IT інфраструктури для типової компанії SMB сегменту.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Безпека малого та середнього бізнесу [Електронний ресурс]: Режим доступу: https://www.kingston.com/ua/blog/data-security/how-to-close-the-security-gap-for-sme

2. Загрози кібербезпеки бізнесу [Електронний ресурс]: Режим доступу: https://itez.com.ua/10-cybersecurity-threats-small-businesses-prevention.html

3. Кібербезпека для малого та середнього бізнесу: зміцнюємо цифрофий периметр [Електронний ресурс]: Режим доступу: https://blog.acer.com/ua/discussion/867/kiberbezpeka-dlya-malogo-ta-serednogo-biznesu-zmicnyuyemo-cifroviy-perimetr

4. Вас атакують хакери: що робити з цим фактом? [Електронний ресурс]: Режим доступу: https://techexpert.ua/the-best-cyber-security-for-company/

5. Страхування кібер-ризиків [Електронний ресурс]: Режим доступу: https://forinsurer.com/news/23/02/20/42397

6. Організація IT-інфраструктури: визначення, типи та функції [Електронний ресурс]: Режим доступу: https://onecloudplanet.com/blog/article/organization-of-it-infrastructure-definition-types-and-functions

7. IT інфраструктура [Електронний ресурс]: Режим доступу: https://koeebox.com/ua/terminy-i/it-infrastruktura/

8. Загрози в бізнесі [Електронний ресурс]: Режим доступу: https://eba.com.ua/top-10-zagroz-kiberbezpetsi-biznesu-u-2023-rotsi/

9. Основи кібергігієни для роботи в інтернеті, робочому та особистому середовищі [Електронний ресурс]: Режим доступу: https://nt.ua/courses/it-management/nt-csf-for-non-it

10. Кібербезпека бізнесу це не лише технічні заходи [Електронний ресурс]: Режим доступу: https://legalitgroup.com/kiberbezpeka-biznesu-tse-ne-lishe-tehnichni-zahodi/

11. Основи кібергігієни [Електронний ресурс]: Режим доступу: https://osvita.diia.gov.ua/courses/lesson/seria-1-vazlivist-ludskogo-faktoru-v-sistemi-bezpeki-vidi-hakerskih-atak-viznacenna-ponatta-kibergigiena

12. Надійний захист RDP: як уникнути атак з використанням паролів [Електронний ресурс]: Режим доступу: https://www.eset.com/ua/about/newsroom/blog/business-security/nadezhnaya-zashchita-rdp-kak-izbezhat-atak-s-ispolzovaniyem-paroley/

13. Віддалена робота: перевірені способи безпеки [Електронний ресурс]: Режим доступу: https://techexpert.ua/remote-work-security-recommendations/

14. Продукти та рішення Bakotech [Електронний ресурс]: Режим доступу: https://bakotech.ua/vendor/tenable-network-security/

15. Що таке пентест – тест на проникнення? [Електронний ресурс]: Режим доступу: https://datami.ua/shho-take-pentest-test-na-proniknennya/

16. Kali Linux для початківців [Електронний ресурс]: Режим доступу: https://timeweb.com/ru/community/articles/kali-linux-dlya-nachinayushchih

17. Про дистрибутив Kali Linux та кібербезпеку [Електронний ресурс]: Режим доступу: https://foxminded.ua/kali-linuks/

18. Мінімізуйте ризики і втрати від злому [Електронний ресурс]: Режим доступу: https://techexpert.ua/it-services/it-bezpeka/

19. Кібербезпека в бізнесі: як уникнути вразливостей та захистити дані? [Електронний ресурс]: Режим доступу: https://netwave.ua/cybersecurity-in-business/

20. Вертузаєв М. С. Захист інформації в комп'ютерних системах від несанкціонованого доступу : навч. посіб. / М. С. Вертузаєв, О. М. Юрченко ; за ред. С. Г. Лаптєва. – Київ : Вид-во Європ. ун-ту, 2021. – 321 с.

21. Ходаков В. Є. Методи і способи захисту інформації // Вступ до комп’ютерних наук : навч. посіб. / В. Є. Ходаков, Н. В. Пилипенко, Н. А. Соколова

22. ; М-во освіти і науки України, Херсон. держ. тех. ун-т. – Київ, 2005. – С. 337–340.

23. Васильєв Ю. Класифікація та аналіз загроз інформаційній безпеці в ключових системах інформаційної інфраструктури. Правове, нормативне та

метрологічне забезпечення системи захисту інформації в Україні, вип. 1 (29), 2015 р. С.56-61.

24. Баловсяк Н. Як зберегти дані/ Н. Баловсяк // Діловодство та документообіг. – 2015. – № 7. – С. 62–73.

25. Балакін С.В. Методи та засоби підвищення достовірності ідентифікації несанкціонованих дій та атак в комп'ютерній мережі : дис. … канд. техн. наук / Балакін С.В. ; Нац. авіа. ун-т. – 2018. – 151 с.

26. Городецька, О. С. Комп'ютерні мережі : навчальний посібник / О. С. Городецька, В. А. Гикавий, О. В. Онищук. − Вінниця : ВНТУ, 2017. − 129 с.

27. Юдін О. К. Захист інформації в мережах передачі даних:підруч./ Г.Ф. Коханович, О. Г. Корченко, О. К. Юдін. – К.:Вид-во ТОВ НВП «ІНТЕРСЕРВІС», 2009. – 215с.

28. Тимошенко А. О. Методи аналізу та проектування систем захисту інформації: курс лекцій / А.О. Тимошенко. – К. : Політехніка, 2007. – 174 с.

29. Девянін. П.Н. Теоретичні основи комп'ютерної безпеки: посібник для ВУЗів / П. Н. Девянін. – М. : Радіо та зв'язок, 2017. – 125 с.

30. Боднар І. Інформаційна безпека як основа національної безпеки. Механізм регулювання економіки, 2014, № 1. С 68-75.

31. Ільченко Н. В. Безпека спілкування через Інтернет / Н. В. Ільченко // Безпека життєдіяльності. – 2019. – № 11. – С. 27.

32. Вертузаєв М. С. Захист інформації в комп'ютерних системах від несанкціонованого доступу : навч. посіб. / М. С. Вертузаєв, О. М. Юрченко ; за ред. С. Г. Лаптєва. – Київ : Вид-во Європ. ун-ту, 2021. – 321 с.

33. Хемфрі Е. Діяльність з кібер-безпеки. Рішення для бізнесу / Е. Хемфрі // Стандартизація, сертифікація, якість. – 2013. – № 1. – С. 16-18.

34. Нестеренко Г. Інформаційна безпека: курс лекцій. Київ: НАУ, 2022. 102 с.

35. Корчак Ю. Сучасні методи та засоби захисту інформації / Ю. Корчак, Ю. Фургала, Л. Корчак // Електроніка та інформаційні технології : зб. наук. пр. /

Львів. нац. ун-т ім. І. Франка ; [редкол.: І. Болеста та ін]. – Львів, 2017. – Вип. 8. – С. 3–17.

36. Коженевський С. Р. Термінологічний довідник з питань технічного захисту інформації / С. Р. Коженевський, Г. В. Кузнецов, В. О. Хорошко, Д. В. Чирков. – К. : ДУІКТ, 2007. – 365 с.

37. Богуш В. М. Інформаційна безпека держави / В. М. Богуш, О. К. Юдін, – К. : МК-Прес, 2005. – 321 с.

38. Боднар І. Інформаційна безпека як основа національної безпеки. Механізм регулювання економіки, 2014, № 1. С 68-75.

39. Васильєв Ю. Класифікація та аналіз загроз інформаційній безпеці в ключових системах інформаційної інфраструктури. Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні, вип. 1 (29), 2015 р. С.56-61

40. Кузнецов О. О. Захист інформації в інформаційних системах : навч. посіб. Х. : ХНЕУ, 2018. – 510 с.

41. Гуз А.М., Довгань О.Д., Марущак А.І. Організація захисту інформації з обмеженим доступом. - К. : Наук.-вид. відділ НА СБ України, 2015. - 378 с.

42. Буров Є. В. Комп'ютерні мережі : підручник. Т. 2 / Є. В. Буров, М. М. Митник ; за заг. ред. В. В. Пасічника. – Львів : Магнолія 2006, 2020. – 204 с. – (Комп'ютинг).

ДОДАТОК А

Короткий звіт подібності