МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ТЕРНОПІЛЬСЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
ІМЕНІ ІВАНА ПУЛЮЯ
ФАКУЛЬТЕТ КОМП'ЮТЕРНО-ІНФОРМАЦІЙНИХ СИСТЕМ І ПРОГРАМНОЇ ІНЖЕНЕРІЇ

КАЛИНИЧЕНКО БОГДАН ЛЮБОМИРОВИЧ

УДК 004.056

Дослідження вразливостей мережі офісу «ZoomSupport» та методів їх усунення

Спеціальність 125 «Кібербезпека»

Автореферат

дипломної роботи на здобуття освітньо-кваліфікаційного рівня «магістр»

Тернопіль — 2019

Роботу виконано на кафедрі кібербезпеки Тернопільського національного технічного університету імені Івана Пулюя

Керівник роботи: доктор фізико-математичних наук, доцент
Грод Іван Миколайович
Тернопільський національний технічний університет імені Івана Пулюя,

Рецензент: Кандидат фізико-математичних наук, професор, завідувач кафедри інформатики та математичного моделювання
Михайлишин Михайло Стахович
Тернопільський національний технічний університет імені Івана Пулюя,

Захист відбудеться 23 грудня 2019 р. о 9.00 годині на засіданні екзаменаційної комісії №32 у Тернопільському національному технічному університеті імені Івана Пулюя за адресою: 46001, м. Тернопіль, вул. Руська, 56, навчальний корпус №1, ауд. 806.

ЗАГАЛЬНА ХАРАКТЕРИСТИКА РОБОТИ

Актуальність дослідження. Комп’ютерні мережі, де протікають персональні чи службові данні, повинні бути захищенні і нема мати вразливостей. У разі появи вразливостей швидко їх ліквідувати, мінімізуючи витоки збереженої персональної інформації клієнтів на зовні. Мережа повинна відповідати сучасним вимогам стійкості до можливих атак і загроз.

Дана робота є актуальною, так як:

-на ринку інформаційних технологій існує потреба в виявленні раніше невідомих атак, так як вони з'являються з великою швидкістю;

-системи виявлення вторгнення стають все більш популярними і їх застосування повинно бути досліджено;

-методи виявлення мережевих загроз та способи їх усунення постійно оновлюються, а мережі розвиваються, а отже потребують оптимізації та вдосконалення.

Мета і завдання дослідження. Провести аналіз мережі офісу ZoomSupport та вразливостей, та запропонувати заходи, які необхідно провести для покращення здатності протистояти потенційним загрозам.

Об’єктом дослідження є комп’ютерна мережа офісу ZoomSupport.

Предметом дослідження є методи виявлення вразливостей в мережі.

Методи дослідження. В процесі дослідження використано загальнонаукові методи пізнання: порівняння, системний аналіз, моделювання. Досліджувалися методи виявлення вразливостей на основі статичного аналізу, активних спроб проникнути в мережу, індуктивного висновку, нечіткої логіки, та залучення зовнішніх ресурсів.

Наукова новизна роботи: вдосконалення методу виявлення вразливостей з метою зменшення кількості можливих загроз для мережі та підвищення ефективності її роботи та ліквідації людського фатору.

Практичне значення дослідження полягає наданні рекомендацій щодо покращення роботи мережі офісу Zoomsupport та навчання працівників.

Апробація результатів дипломної роботи. Основні положення дослідження доповідалися й обговорювалися на науково-практичних конференціях: на VII НАУКОВО-ТЕХНІЧНОЇ КОНФЕРЕНЦІЇ «ІНФОРМАЦІЙНІ МОДЕЛІ, СИСТЕМИ ТА ТЕХНОЛОГІЇ » (Тернопіль, 11-12 грудня 2019 року).

Структура роботи. Дипломна робота складається із вступу, шести розділів, висновків, списку використаних джерел із найменувань. Робота містить 18 рисунків, 2 таблиці і 4 формули. Обсяг основного тексту становить 75 сторінок, перелік використаних джерел 17 сторінка, додатки 2 сторінок. Загальний обсяг дипломної роботи складає 77 сторінок.

ОСНОВНИЙ ЗМІСТ РОБОТИ

У вступі обґрунтовано актуальність проблеми, визначено об’єкт і предмет дослідження, сформульовано його мету, завдання, розкрито теоретичну та методологічну основу, методи дослідження; висвітлено наукову новизну, практичне значення роботи;.

У першому розділі — *“Забезпечення безпеки в комп’ютерних мережах”* — проаналізовано визначення поняття загроз та вразливостей, коротко описано причини їх виникнення. Розглянуті проблеми автентифікації користувачів, налаштування фаєрволів, протоколи SSL та мережі VLAN. Розглянуто методи виявлення вразливостей різних типів: апаратних, програмних та людський фактор.

У другому розділі — *“Дослідження вразливостей мережі та продукту компанії”* — було описано будову мережі офісу ZoomSupport та описано як відбувається доступ до ресурсів в самій мережі. Описано роботу Active Directory та Hypervisor.

У третьому розділі − “***Отримання несанкціонованого доступу до мережі методом фішингу***»”− детально описано та проаналізовано процес внутрішньої фішингової атаки та її результати. Також оппписано результат захисту від зовнішньої фішингової атаки на мережу офісу.

ВИСНОВКИ

У дипломній роботі було запропоновано вирішення до проблеми захисту від вразливостей в мережі, а саме через методи проведення регулярного навчання робочого персоналу компанії.

1) проведено огляд джерел в області дослідження;
2) виконано аналіз сучасних методів виявлення вразливостей мереж. Проведено порівняння існуючих методів, яке показало, що на рівні мережі, без людського фактору проникнути не можливо. У зв'язку з цим подальше дослідження було зосередженне на людському факторі мережі..
3) запропоновано вдосконалений метод навчання персоналу та його регулярне проведення;
4) протестовано ефективність роботи вдосконаленого методу;
5) проаналізовано сучасні технологічні рішення для розробки захисту мереж;
6) доведено економічну доцільність розробки;

З практичної точки зору запропонований алгоритм може бути використаний для інтегрування в існуючу систему навчання персоналу. Аналіз проведення перших тренінгів показав кращі результати, між персоналом, щодо IT-secutiry обізнаності, ніж були попередні. Вдосконалена система навчання має певні обмеження, що і може бути предметом подальших досліджень.

АНОТАЦІЯ

Ключові слова: МЕРЕЖА, МЕТОДИ ВИЯВЛЕННЯ ВРАЗЛИВОСТЕЙ, СИСТЕМИ ВИЯВЛЕННЯ ВТОРГЕНЬ, НАВЧАННЯ, VLAN, SSL, ACTIVE DIRECTORY

Об'єкт дослідження: комп’ютерна мережа офісу ZoomSupport

Мета роботи (проекту): Провести аналіз мережі офісу ZoomSupport та вразливостей, та запропонувати заходи, які необхідно провести для покращення здатності протистояти потенційним загрозам Методи дослідження: аналіз, системний підхід, методи: статистичні, контрольованого навчання, неконтрольованого навчання, на основі щільності розподілу набору даних, кластеризації та класифікації.

У спеціальній частині детально описано та проаналізовано процес внутрішньої фішингової атаки та її результати. Також опписано результат захисту від зовнішньої фішингової атаки на мережу офісу В економічному розділі визначено економічну ефективність від розробки і реалізації запропонованого алгоритму.

Практичне значення роботи полягає в можливості інтеграції розробленого алгоритму в існуючу систему виявлення аномалій для покращення ефективнотсі проведення навчання персоналу.

Результати проведених в дипломній роботі досліджень можуть бути використані для подальшої роботи над удосконаленням систем розробки захищенних мереж.

Наукова новизна дослідження полягає в вдосконалення методу виявлення вразливостей з метою зменшення кількості можливих загроз для мережі та підвищення ефективності її роботи.

ANOTATION

Keywords: NETWORK, VULNERATION METHODS, EMERGENCY DETECTION SYSTEMS, TRAINING, VLAN, SSL, ACTIVE DIRECTORY

Object of Study: The ZoomSupport Office Computer Network

Purpose of the project: To analyze the ZoomSupport office network and vulnerabilities, and to suggest measures that need to be taken to improve the ability to withstand potential threats. data, clustering, and classification.

The special part describes and analyzes in detail the process of internal phishing attack and its results. The result of protection against external phishing attack on the office network is also described. The economic section defines the economic efficiency from the development and implementation of the proposed algorithm.

The practical value of the work lies in the possibility of integrating the developed algorithm into the existing anomaly detection system to improve the efficiency of staff training.

The results of the research carried out in the thesis can be used to further work on improving the systems of development of secure networks.

The scientific novelty of the research is to improve the method of vulnerability detection in order to reduce the number of possible threats to the network and increase its efficiency.