Секція 1

РОЗРОБКА ТЕХНОЛОГІЇ ВИЯВЛЕННЯ ВРАЗЛИВОСТЕЙ В КОРПОРАТИВНІЙ ІНФОРМАЦІЙНІЙ СИСТЕМІ

Бутенко С. І.
Національний аерокосмічний університет ім. М. Є. Жуковського «ХАІ»
Науковий керівник: Пєвнєв В. Я.

Актуальність. Корпоративні інформаційні системи (КІС) стали невід'ємною складовою сучасного бізнесу, прискорюючи його розвиток та полегшуючи управління багатьма процесами. Проте, зростання комплексності КІС породжує загрозу вразливостей, які можуть призвести до незаконного доступу до інформації, порушення конфіденційності та цілісності даних. Тому розробка технології виявлення вразливостей в корпоративній інформаційній системі є актуальною та важливою задачею. Корпоративні інформаційні системи великих компаній регулярно зазнають змін - оновлюється конфігурація обладнання, змінюється топологія мереж, з'являються нові вузли і цілі системи [1].

На сьогодні не існує єдиного алгоритму виявлення вразливостей в корпоративних інформаційних системах. Подібна ситуація виникає через те, що кожна з досліджуваних систем має свої особливості та потребує індивідуального підходу [2]. Тому розробка технології виявлення вразливостей стає надзвичайно важливою задачею для забезпечення безпеки корпоративних інформаційних систем.

Метою є дослідити існуючі підходи до виявлення вразливостей в корпоративних інформаційних системах та визначити вимоги до технології, що буде розроблятися.

Основні положення. Розглядаючи найрозповсюджені типи загроз, що виникають в інформаційних системах можна виділити рад тих, що зустрічаються найчастіше: Недоліки захисту службових протоколів, словникові паролі, недостатній рівень захисту привілейованих облікових записів, зберігання важливої інформації у відкритому вигляді, вразливі версії програмного забезпечення, недостатня освіченість персоналу системи з приводу можливих дій зловмисників [3]. Виходячи з описаного висче можна зазначити, що джерелом більшості з описаних загроз є недбалість персоналу системи на етапі її створення або обслуговування.

У доповіді розглядаються різні підходи для виявлення вразливостей та різні підходи. Більшість з них потребує використання в комплексі з іншими та під керуванням досвідченого експерта. Основні з низ подані нижче.

Сканування вразливостей. Це процес автоматичного сканування мережі та систем на наявність вразливостей. Існують спеціальні програмні засоби які виявляють вразливості, аналізуючи порти, служби, програмне забезпечення та конфігурації систем.

Аудит безпеки. Це процес систематичного перевірки безпеки системи, включаючи перевірку наявності вразливостей. Він включає огляд конфігурацій, перевірку політик безпеки, перевірку прав доступу, аналіз журналів подій та інші процедури.

Пенетраційне тестування. Це процес активного тестування системи шляхом моделювання атак та спроб проникнення з боку зловмисників.

Моніторинг безпеки. Це неперервне спостереження за системою з метою виявлення потенційних вразливостей або зловмисної діяльності. автоматизовані системи управління вразливостями.

Висновки. Виявлення вразливостей корпоративних інформаційних систем потребує комплексного підходу з урахуванням особливостей конкретної досліджуваної системи. Будь який процес виявлення вразливостей в даному типі систем є сильно залежним від рівня допуску до компонентів, що надається особі, що проводить аналіз, та її рівня експертності. Важливим є те, щоб експерт, що проводить аналіз корпоративної інформаційної системи компанії, яка працює в певній галузі мав високий рівень досвідченості не лише в принципах побудови систем безпеки, а й особливостях даної галузі.

Не існує конкретних стандартизованих алгоритмів виявлення вразливостей через те, що кожна система має власні особливості, які важко урахувати в стандартизованому алгоритмі. Можуть бути використані комплексні підходи на базі методик аналізу. Але набір інструментів буде відрізнятися в залежності від обраної системи та вимог до рівня безпеки.

Список літератури

1. Дмитро Мехед, Юлія Ткач, Володимир Базилевич, Володимир Гур'єв, Ярослав Усов. АНАЛІЗ ВРАЗЛИВОСТЕЙ КОРПОРАТИВНИХ ІНФОРМАЦІЙНИХ СИСТЕМ. *Jrnl.* URL – https://jrnl.nau.edu.ua/index.php/ZI/article/view/12453/17051(дата звернення: 01.06.2023);
2. А.І. Андрухів, Д.О. Тарасов. Порівняння методів оцінки захищеності корпоративних інформаційних систем. *Lpnu.* URL – https://science.lpnu.ua/sites/default/files/journal-paper/2017/dec/7287/013-9vis573.pdf (дата звернення: 01.06.2023);
3. Вразливості корпоративних інформаційних систем, 2019. *Ptsecurity.* URL – https://www.ptsecurity.com/ru-ru/research/analytics/corporate-vulnerabilities-2019/#id1 (дата звернення: 01.06.2023).

Відомості про авторів

Бутенко Сергій Ігорович, студент кафедри комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», s.butenko@student.csn.khai.edu
Пєвнєв Володимир Яковлевич, професор кафедри комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», д.т.н., доцент, v.pevnev@csn.khai.edu