УДК 004.7

Колощук М. С., магістрантка, гр. КБм-21-1,
Науковий керівник: Єфіменко А. А., канд. техн. наук,
доцент, зав. кафедри КІ та КБ,
Вакалюк Т. А., д-р пед. наук, професор, професор кафедри ІПЗ
Державний університет «Житомирська політехніка»

ПОШИРЕНІ ТИПИ МЕРЕЖЕВИХ АТАК

Мережеві загрози та атаки можуть перешкоджати безпеці мережі та додаткам. Крім того, оскільки люди стають все більш залежними від цифрових комунікаційних технологій, поширені типи мережевих атак зростають. Одні з най поширених загроз і атак описані нижче.

1. Комп'ютерний вірус. Комп'ютерний вірус є однією з найпоширеніших атак на мережу, яка може завдати значної шкоди даним.

Тип зловмисного програмного забезпечення, це унікальні фраг-менти коду, які можуть спричиняти хаос і поширюватися з комп'ютера на комп'ютер. Зараження шкідливим програмним забезпеченням досить поширене, і вірусоподібний троянський кінь може серйозно пошкодити мережу. Якщо відкрити електронний лист зі шкідливим посиланням або завантажити посилання із заражених веб-сайтів, ці віруси можуть пошкодити ваші файли, заразити інші комп'ютери та викрасти особисту інформацію [1].

2. Шкідливе програмне забезпечення. Одним з найнебезпечніших кіберзлочинів, які можуть завдати величезної шкоди, є атака зловмисного програмного забезпечення. Хакери намагаються отримати несанкціонований доступ до цільової системи та порушити або пошкодити файли та дані за допомогою шкідливих кодів, а точніше шкідливим програмним забезпеченням. Крім того, це може впливати як на внутрішні, так і на зовнішні кінцеві пристрої мережі [1].

3. Мережевий хробак. Мережеві хробаки – це не що інше, як шкідливе програмне забезпечення, яке поширюється з одного зараженого комп'ютера на інший шляхом копіювання. Вони досягають своїх цілей, використовуючи вразливості мережі. Більше того, це може вплинути на вашу систему без будь-якої допомоги сторонніх користувачів [1].

4. Фішинг. Ще одним поширеним типом атаки на безпеку мережі є фішинг, який є формою атаки соціальної інженерії. Кіберзлочинці обманом змушують користувачів натиснути на шахрайське посилання електронної пошти або повідомлення, яке виглядає законним. Отже, коли користувачі натискають посилання, зловмисне програмне забезпечення завантажується в їхні телефони або системи, що дозволяє хакерам викрасти конфіденційні дані або інформацію, наприклад номери кредитних карток або банківські паролі [2].

5. Ботнет. Ботнети – це мережа зламаних систем, підключених до Інтернету. Хакер отримує доступ до всіх цих пристроїв у мережі і маніпулює ботами, щоб розсилати спам, здійснювати крадіжку даних і вмикати DDoS-атаки (розподілена відмова в обслуговуванні) [1].

6. MIM. Ще одна форма мережевих загроз виникає внаслідок атак MIM (man-in-the-middle). У цьому типі кібератаки хакери викрадають приватне спілкування, призначене між двома сторонами. Перехоп-люючи інформацію, зловмисник намагається контролювати та пере-направляти їхні повідомлення, щоб вкрасти конфіденційні дані або шпигувати за жертвами [1].

7. DoS і DDoS-атаки. Атака на комп'ютерну мережу, що має на меті зробити комп'ютерні ресурси недоступними для користувачів через перевищення припустимих меж функціонування мережі, операційної системи або додатка; підвищення витрат ресурсів процесора та зменшення пропускної здатності каналу зв'язку [3].

8. Програми-вимагачі. Програма-вимагач – це шкідливе програмне забезпечення, яке хакери шифрують усі файли в цільових системах, мережах і серверах. Інші кампанії-вимагачі можуть отримати доступ до мережі та блокувати файли, поки не буде сплачений викуп в обмін на ключ дешифрування, використовуючи слабкі паролі та інші вразливі місця [1].

9. Атаки на 5G. Атаки на 5G є більш просунутою формою загрози безпеці мережі. Хоча мережі 5G забезпечують високу швидкість передачі даних, це також підвищує ризик кібератак. Хакери атакують кілька систем, мобільних пристроїв та мережі IoT (Інтернет речей), використовуючи пристрої 5G для розгортання атак на безпеку мережі. Зловмисник також може вносити зміни в режимі реального часу [4].

10. SQL Injection. SQL Injection є одним із найпоширеніших векторів атак, які хакери використовують для крадіжки даних. Цей тип мережевої атаки поширений на погано розроблені програми та веб-сайти. Оскільки вони містять уразливі поля для введення користувачів (наприклад, сторінки пошуку та входу, форми запитів на продукти та підтримку, область коментарів тощо), хакери можуть легко зламати, змінивши сценарії.

Атака з ін'єкцією SQL є серйозною загрозою та одним із основних векторів атак, які використовують хакери. Більше того, він може легко заразити або експлуатувати будь-який веб-сайт, який використовує базу даних на основі SQL [1].

Питання безпеки завжди стояло перед комп'ютерними мережами, але сьогодні як ніколи зростає усвідомлення того, наскільки важливою є безпека комп'ютерних мереж.

Список використаних джерел

1. Грайворонський М. В., Новіков О. М. Безпека інформаційно-комунікаційних систем. Київ: Видавнича група BHV, 2009. 608 с.

2. Сабадаш В. П. Фішинг як найбільш розвинений вид шахрайства в Інтернеті. Хмельницький: Університетські наукові записки, 2006. С. 228-233.
3. Бурячок В. Л., Толубко В. Б., Хорошко В. О., Толюпа С. В. Інформаційна та кібербезпека: соціотехнічний аспект: підручник. Київ: ДУТ, 2015. 288 с.
4. Philippe Z Lin, Charles Perine, Rainer Vosseler Attacks From 4G/5G Core Networks. Institute of Information Industry, 2021. 64 c.