Боровський О. І., магістрант,
Державний університет «Житомирська політехніка»

МОНІТОРИНГ ТА ВИЯВЛЕННЯ АНОМАЛІЙ У WI-FI МЕРЕЖАХ

WI-FI мережі стали неодмінною складовою нашого повсякденного життя, забезпечуючи зручний та швидкий доступ до Інтернету. Збільшення кількості підключених пристроїв також підвищує ризик кіберзагроз, тому моніторинг та виявлення аномалій стає ключовою стратегією безпеки WI-FI.

Аномалії у WI-FI мережах можуть мати різноманітні прояви, і їх виявлення вимагає уважного аналізу та розуміння нормальної поведінки мережі. Ось детальніший огляд аспектів, які можуть вказувати на потенційні проблеми:

- Низька швидкість передачі даних може бути симптомом багатьох проблем, включаючи перевантаження мережі, інтерференцію сигналу, або навіть несанкціонований доступ до мережі;
- Нестабільне підключення часто є результатом фізичних перешкод, таких як стіни або інші великіоб'єкти, що блокують сигнал, або може бути викликано програмними збоями;
- Проблеми з безпекою можуть включати слабкі паролі, застаріле програмне забезпечення, або вразливості в аппаратному забезпеченні, які можуть бути використані зловмисниками;
- Проблеми з налаштуваннями можуть виникати через помилки при конфігурації мережі або неправильне управління доступом до мережі;
- Проблеми з обладнанням можуть бути пов'язані з фізичними пошкодженнями або зносом обладнання, що вимагає заміни або ремонту.

Виявлення аномалій у WI-FI мережах – це процесс ідентифікації та реагування на незвичайні або підозрілі активності, які можуть вказувати на потенційні загрози або несправності. Це може включати:

- Аналіз журналів реєстрації подій, що дозволяє виявити незвичайні входи абоспроби доступу до мережі;
- Аналіз пакетів для перевірки даних, які передаються через мережу, на предмет шкідливого вмісту або незвичайних патернів;
- Моніторинг мережевих потоків для виявлення несподіваних змін у трафіку або незвичайно великих обсягів передачі даних.
- Аналіз маршрутів для виявлення змін у маршрутизації, які можуть вказувати на спроби перехоплення даних;
- Кореляційний аналіз IP-адрес для ідентифікації підозрілих зв'язків між пристроями та мережевими вузлами.

Для цього можна використовувати різноманітні програмні та апаратні комплекси:

- Wireshark: Це один з найбільш відомих інструментів для аналізу мережевого трафіку. Він дозволяє перехоплювати та аналізувати пакети даних, що пересилаються по WI-FI мережі, і виявляти будь-які аномальні патерни або активності;
- Kismet: Це програмне забезпечення для моніторингу та виявлення аномалій у WI-FI мережах. Воно дозволяє здійснювати сканування навколишніх мереж, аналізувати трафік і виявляти потенційні загрози;
- Snort: Це система виявлення вторгнень (IDS), яка може бути використана для моніторингу трафіку у WI-FI мережі та виявлення аномалій, які можуть свідчити про кіберзагрози;
- Aircrack-ng: Це набір інструментів для тестуваннябезпеки WI-FI мереж, але він також може використовуватися для виявлення аномалій. Він дозволяє аналізувати трафік, виявляти слабкі точки безпеки і виявляти незвичайну активність;
- Netcut: Це програмне забезпечення для Windows, яке дозволяє вам перевіряти та керувати мережевим трафіком у WI-FI мережі. Воно може допомогти виявити незвичайну активність або несанкціонованих користувачів у мережі.

Забезпечення безпеки WI-FI мереж вимагає постійного вдосконалення технологій та методів моніторингу, а також освіти користувачівщо докращих практик безпеки. Дотримання найновіших тенденцій у цій області є ключовим для забезпечення надійного функціонування WI-FI мереж та захисту їх від потенційних кіберзагроз.

Список використаних джерел

1. Виявлення аномалій у мережевій поведінці [Електронний ресурс]. Режим доступу до ресурсу: https://cutt.ly/0w3YnORF
2. Tyler Wrightson "Wireless Network Security: A Beginner's Guide", McGraw Hill; 1st edition 2012. – 368с.
3. Андрєєв В.І., Хорошко В.О., Чередниченко В.С., Шелест М.Є. Основи інформаційної безпеки; за ред. В.О. Хорошка. –[2-евид.]. –К.: Вид. ДУІКТ, 2009. – 292 с.