**УДК 004.78**

Методи моніторингу мережевого трафіку з метою виявлення та блокування зовнішнього вторгнення в комп'ютерні системи

Борщ Андрій Андрійович,

здобувач вищої освіти освітнього ступеня «Магістр», 2 курс

Національний авіаційний університет

м. Київ, Україна

6171908@stud.nau.edu.ua

**Висоцька Олена Олександрівна,**

к.т.н., доцент кафедри Кібербезпеки

**Вступ. / Introductions.** Сьогодні Інтернет став не лише інструментом для передачі даних, але й середовищем для здійснення кібератак, зокрема вторгнень у комп'ютерні системи, DDoS-атак та інших форм зловмисної активності. Рівень мережевих загроз постійно зростає, стаючи дедалі складнішими та небезпечнішими. Підприємства, державні установи та приватні користувачі щодня стикаються з ризиками, пов'язаними з витоками даних, руйнуванням інфраструктури та порушенням конфіденційності інформації.

**Мета роботи. / Aim.** Моніторинг мережевого трафіку є ключовим аспектом забезпечення безпеки інформаційних систем. Сучасні системи безпеки мають бути здатними не лише виявляти зовнішні загрози, але й ефективно блокувати їх для забезпечення стабільної роботи комп'ютерних мереж. Дані аспекти вимагають дослідження існуючих можливостей впровадження інноваційних підходів, таких як поведінковий аналіз і машинне навчання для запровадження швидкої реакції на аномалії у мережевому трафіку.

**Виклад основного матеріалу дослідження/ Summary of the main research material.** Методи моніторингу мережевого трафіку можна розділити на кілька ключових категорій, кожна з яких має свої особливості та призначення. Найбільш поширеними є [1]:

1. Сигнатурний аналіз, що працює на основі порівняння мережевого трафіку з базою відомих сигнатур атак. Система шукає збіги між вхідним або вихідним трафіком і шаблонами, характерними для відомих атак. Основна перевага сигнатурного аналізу полягає в його швидкості та простоті реалізації, але його недолік – нездатність виявляти нові або модифіковані загрози, для яких сигнатур ще не існує.

2. Поведінковий аналіз, що полягає в тому, що система вивчає типову поведінку мережі, визначаючи, які дії є нормальними для певного середовища. Аномалії, такі як раптове зростання трафіку або незвичайні запити, можуть свідчити про потенційні загрози. Цей метод дозволяє виявляти нові типи атак, але може генерувати велику кількість хибнопозитивних спрацювань, оскільки зміни в легітимній поведінці можуть бути помилково ідентифіковані як загроза.

3. Алгоритми машинного навчання, що можуть аналізувати великі обсяги даних, знаходити закономірності й автоматично ідентифікувати аномалії, які вказують на потенційні загрози. Цей метод поєднує в собі переваги сигнатурного та поведінкового аналізу, але вимагає великих обчислювальних ресурсів і точних налаштувань для мінімізації хибнопозитивних спрацювань.

4. Аналіз потоків NetFlow, що полягає в аналізі потоків даних, які проходять через мережеве обладнання. Він дозволяє збирати інформацію про джерела, призначення, обсяг і типи переданих даних. NetFlow допомагає виявляти DDoS-атаки та інші форми аномальної активності, використовуючи статистику потоків, а не самі пакети.

Ефективне виявлення та блокування зовнішніх вторгнень у комп'ютерні системи забезпечується завдяки впровадженню спеціалізованих програмних рішень. Серед найбільш поширених систем для моніторингу мережевого трафіку та виявлення вторгнень можна виділити такі [2]:

1. Snort – це одна з найбільш відомих систем виявлення вторгнень, яка використовує сигнатурний підхід для аналізу мережевого трафіку. Snort здатен виявляти різні типи атак, такі як сканування портів, атаки на рівні додатків, атаки типу DDoS та інші. Однак його ефективність залежить від актуальності бази сигнатур.

2. Suricata – це багатофункціональна система для моніторингу мереж, яка підтримує сигнатурний аналіз, поведінкове виявлення аномалій і аналіз HTTP-трафіку. Suricata також здатна працювати у режимі виявлення вторгнень (IDS) або запобігання (IPS), що робить її гнучким інструментом для захисту мереж.

3. Zeek (Bro) – це система аналізу мережевого трафіку, орієнтованою на глибокий аналіз подій, що відбуваються в мережі. Вона здатна визначати складні атаки завдяки комбінуванню поведінкового аналізу і кореляції подій. Zeek забезпечує детальний журнал подій, що дозволяє аналізувати загрози на більш глибокому рівні, ніж звичайні IDS.

4. Wireshark – це потужний інструмент для аналізу мережевих пакетів у реальному часі. Він дозволяє детально досліджувати трафік і виявляти аномалії або вторгнення на рівні окремих пакетів. Хоча Wireshark зазвичай використовується для глибокого аналізу, а не для безперервного моніторингу, його часто застосовують для розслідування після інцидентів.

5. PRTG – це комплексне рішення для моніторингу мереж, яке включає функції збору статистики, виявлення аномалій і виявлення вторгнень. PRTG підтримує аналіз трафіку за допомогою технологій SNMP, NetFlow, jFlow та sFlow, що дозволяє отримувати повну картину мережевої активності.

Одним із підходів до виявлення та блокування зовнішнього трафіку без використання сторонніх систем є розробка вбудованої системи моніторингу, яка базується на гнучкому аналізі трафіку і самостійних рішеннях для захисту на рівні внутрішньої мережевої інфраструктури. Такий метод передбачає використання власних програмних рішень, інтегрованих безпосередньо в існуючу мережеву архітектуру. Основна ідея полягає в тому, щоб мережеві пристрої або сервери самостійно аналізували трафік і приймали рішення щодо його блокування без залучення зовнішніх систем захисту, таких як хмарні сервіси або сторонні інструменти.

Проведений аналіз дозволяє визначити основні компоненти системи моніторингу мережевого трафіку:

1. Аналізатор потоків трафіку – відповідає за збір і аналіз мережевого трафіку в режимі реального часу та працює на рівні маршрутизаторів, комутаторів і серверів, де збирається інформація про всі вхідні та вихідні пакети, їхні джерела, призначення, розмір та тип даних. Використовуючи попередньо задані правила і політики, аналізатор фіксує підозрілі патерни поведінки, такі як незвично велика кількість запитів до одного порту, спроби сканування або підозрілі підключення з невідомих IP-адрес.

2. Модуль виявлення аномалій – використовує методи поведінкового аналізу для визначення аномальної активності. Важливою характеристикою цього підходу є можливість самостійно навчатися та адаптуватися до змін у мережевому трафіку, щоб постійно вдосконалювати моделі нормальної поведінки. Наприклад, система може відстежувати певні патерни доступу до мережі від конкретних користувачів або серверів і визначати, коли їхня поведінка відхиляється від норми.

3. Автоматизовані правила блокування – використовує заздалегідь встановлені правила для автоматичного блокування підозрілого трафіку. Наприклад, якщо система виявляє підозрілу активність із певної IP-адреси, вона може тимчасово заблокувати цю адресу, запобігаючи подальшим спробам вторгнення. Також система може автоматично ізолювати сегменти мережі, якщо в них виявляється підозріла активність.

4. Локальний журнал подій – містить інформацію про всі виявлені аномалії, заблоковані IP-адреси та загальні статистичні дані щодо мережевого трафіку. Такий журнал може використовуватися як для подальшого аналізу, так і для забезпечення прозорості в процесі реагування на загрози.

Оскільки всі компоненти для моніторингу, виявлення та блокування інтегровані в мережеву інфраструктуру, цей підхід не залежить від зовнішніх постачальників послуг або сторонніх систем безпеки. Це забезпечує додатковий рівень контролю та конфіденційності.

Використання внутрішніх ресурсів для моніторингу та блокування зовнішніх загроз знижує потребу в дорогих зовнішніх рішеннях. Це може бути особливо важливо для невеликих компаній, які не мають можливості інвестувати в складні зовнішні системи безпеки.

**Висновки. / Conclusions.** Моніторинг мережевого трафіку є важливим інструментом для забезпечення безпеки комп'ютерних систем та виявлення зовнішніх загроз. Сучасні методи, такі як сигнатурний та поведінковий аналіз, а також алгоритми машинного навчання, дозволяють виявляти та блокувати атаки на ранніх етапах. Програмні рішення, такі як Snort, Suricata та Zeek, забезпечують ефективне виявлення загроз і захист мереж від вторгнень. Незважаючи на високу ефективність цих методів і інструментів, важливо постійно оновлювати системи безпеки, адаптуючись до нових типів атак і загроз.

Виявлення і блокування зовнішнього трафіку без використання зовнішніх систем є можливим за допомогою власних вбудованих інструментів моніторингу та аналізу трафіку. Такий підхід дозволяє підвищити рівень контролю над мережею, скоротити час реагування на загрози та забезпечити економічну ефективність. Незважаючи на виклики, пов’язані з налаштуванням і підтримкою системи, вона може стати потужним інструментом для захисту мережевої інфраструктури від зовнішніх загроз. Використання внутрішньої системи для виявлення і блокування загроз дозволяє скоротити час між виявленням аномалії і реагуванням на неї. Оскільки всі дії відбуваються всередині мережі, система може швидко реагувати на будь-які загрози без затримок, пов'язаних із передачею даних на зовнішні платформи.

**Список літератури**

1. Методи аналізу та моделювання безпеки розподілених інформаційних систем: навч. посіб. / В.В. Литвинов, В.В. Казимир, І.В. Стеценко та ін. - Чернігів: Чернігівський національний технологічний університет, 2023. - 254 с.

2. Bearden W.O. Marketing Strategies: Insights and Innovations / W. O. Bearden, T. N. Ingram, R. W. LaForge. – 3rd ed. – New York: McGraw-Hill Higher Education, 2015.