УДК 004.056.5

В. ГНЄДОВА, І. ЯРОВА

Національний університет Одеська політехніка

ВДОСКОНАЛЕННЯ ПРОТОКОЛІВ МАРШРУТИЗАЦІЇ В КОРПОРАТИВНИХ МЕРЕЖАХ: ІНТЕЛЕКТУАЛЬНА МАРШРУТИЗАЦІЯ І ЗАХИСТ ВІД DDoS-АТАК

Вступ. Постійне зростання кіберзагроз, особливо таких, як DDoS-атаки, вимагає перегляду та вдосконалення існуючих протоколів маршрутизації в корпоративних мережах. Традиційні протоколи, такі як BGP(Border Gateway Protocol) та OSPF(Open Shortest Path First), не завжди обладнані для ідентифікації та блокування аномального трафіку. Удосконалення їх за допомогою алгоритмів машинного навчання та інтелектуальних функцій може забезпечити надійний захист мереж і значно підвищити їх безпеку.

Мета: проаналізувати можливості вдосконалення протоколів маршрутизації з акцентом на захист від DDoS-атак, запропонувати рішення, що поєднують алгоритми машинного навчання з BGP та OSPF, для підвищення рівня захищеності та ефективності мережі.

1. Інтелектуальна маршрутизація зі захистом від DDoS-атак

Протоколи внутрішньої та зовнішньої маршрутизації, такі як OSPF, BGP відповідно, широко застосовуються у корпоративних мережах, але проблема вбудованих механізмів для ідентифікації та зупинки DDoS-атак досі є актуальною. Це робить протоколи уразливими до масивних потоків аномального трафіку, який перевантажує мережеву інфраструктуру та може призвести до відмови в обслуговуванні критично важливих мережевих ресурсів [1].

Впровадження алгоритмів, що аналізують мережевий трафік на наявність аномалій дозволить додати новий рівень безпеки на другому рівні еталонної моделі OSI або TCP/IP, зупиняючи загрози до того, як вони досягнуть цільових серверів або мережевих пристроїв. Дані алгоритми призначені для аналізу таких параметрів трафіку, як обсяг, швидкість і частоту запитів, крім того, поведінкові характеристики для виявлення підозрілої активності, яка може вказувати на атаку, що відбувається.

Адаптивне блокування аномального трафіку є наступним кроком після виявлення загрози. Воно передбачає розробку функцій автоматичного блокування підозрілих IP-адрес або цілих сегментів мережі без необхідності ручного втручання. На рівні маршрутизатора така функція здатна в реальному часі блокувати джерела шкідливого трафіку, що дозволяє значно знизити навантаження на мережеве обладнання та мінімізувати ризик успішного проникнення. Завдяки даній адаптивності маршрутизатор може не лише миттєво реагувати на загрози, а й аналізувати нові типи атак, що робить систему більш гнучкою та стійкою до нових та непередбачених загроз у майбутньому.

2. Інтелектуальні маршрутизатори з функцією самонавчання

Впровадження алгоритмів машинного навчання у маршрутизатори відкриває нові можливості для забезпечення мережевої безпеки, шляхом аналізу

шаблонів трафіку та автоматичного реагування на потенційні загрози. У даній системі маршрутизатор виконує не тільки функцію передачі даних, а й активно захищає мережу, виявляючи та блокуючи шкідливий трафік в режимі реального часу. Алгоритми аналізують поведінкові шаблони підключень: обсяг переданих даних, швидкість і частоту запитів, джерела трафіку та інші параметри. З їх допомогою маршрутизатор може створювати модель нормальної поведінки для кожного підключення і на основі відхилень від цієї моделі автоматично реагувати на підозрілі з'єднання.

Одним з ключових аспектів є можливість самонавчання маршрутизаторів для прогнозування загроз. Це призводить до того, що маршрутизатор може не лише реагувати на вже відомі шаблони атак, а й адаптуватися до нових видів загроз, що з'являються у мережі. Самонавчання дозволяє маршрутизатору вивчати нові схеми аномальної поведінки, яка може бути ознакою DDoS-атаки або іншої шкідливої діяльності. На основі таких даних він коригує власні налаштування без втручання адміністратора, створюючи більш гнучкий і стійкий захист мережі [2].

Використання машинного навчання дозволяє створити проактивний захист. Тобто маршрутизатор виявляє загрозу ще до того, як атака встигне поширитися, що знижує ризик повномасштабного DDoS-нападу. Крім того, адаптивне блокування забезпечує динамічне корегування фільтрації трафіку, що дозволяє зменшити навантаження на інфраструктуру, оскільки воно блокує підозрілі запити ще до їхнього впливу на систему [2].

Таким чином, впровадження машинного навчання в маршрутизаторах підвищує безпеку мережі, завдяки автоматичному прогнозуванню і адаптації до нових загроз Це робить мережу стійкішою, підвищує ефективність захисту від атак та оптимізує розподіл навантаження на мережеві ресурси, забезпечуючи надійність і стабільність роботи навіть під час спроб зовнішніх атак.

3. Інтеграція інтелектуальних функцій до протоколів маршрутизації

Інтеграція інтелектуальних функцій у протоколи маршрутизації, такі як BGP та OSPF, може суттєво покращити їхню ефективність у захисті корпоративних мереж від DDoS-атак.

По-перше, для впровадження алгоритмів машинного навчання необхідно оновити програмне забезпечення маршрутизаторів, включивши в нього модулі для аналізу трафіку. Це дозволить маршрутизаторам виявляти аномалії та автоматично коригувати маршрути у разі загрози, що гарантує більш високий рівень безпеки.

По-друге, слід створити централізовану базу даних аномалій, до якої будуть підключені всі маршрутизатори. Дана база міститиме інформацію про нові загрози то шаблони аномального трафіку. Встановлення захищених каналів для обміну даними дозволить маршрутизаторам синхронізувати свої знання про загрози в режимі реального часу.

Крім того, важливою є адаптація ML-моделі згідно із специфікою мережі для зменшення кількості хибних спрацювань і підвищення ефективності виявлення загроз [3].

Додатковими кроками є періодичне тестування, тренування та моніторинг

інтегрованої системи, що забезпечать її стабільність та надійність у захисті від кіберзагроз. Дана інтеграція дозволить маршрутизаторам активно реагувати на атаки, забезпечуючи проактивний захист корпоративних мереж.

Висновок. Проведений аналіз дозволяє зробити висновок, що інтеграція інтелектуальних функцій у протоколи маршрутизації, такі як BGP та OSPF, відкриває нові горизонти для підвищення безпеки корпоративних мереж, особливо в умовах зростаючих загроз з боку DDoS-атак. Сучасні методи атак стають дедалі витонченішими, тому традиційні механізми захисту, закладені в існуючи протоколи, вже не відповідають актуальним вимогам безпеки.

Впровадження алгоритмів машинного навчання дозволить маршрутизаторам здійснювати аналіз трафіку в реальному часі, що суттєво покращить їх здатність до виявлення аномалій. Це не лише знизить ймовірність пропуску підозрілих запитів, а й забезпечить автоматичне коригування маршрутів для мінімізації наслідків атак. Самонавчальні моделі, здатні адаптуватись до нових загроз, будуть не лише ідентифікувати аномальний трафік, а й ефективно блокувати його на стадії маршрутизації.

Створення централізованої бази даних аномалій дозволить маршрутизаторам обмінюватись інформацією про нові загрози, що значно підвищить загальний рівень безпеки. Використання захищених каналів для синхронізації даних між маршрутизаторами та базою даних гарантує, що інформація про загрози буде актуальною та доступною в будь-який момент. Таким чином підвищується швидкість реагування на нові загрози і стійкість мережі до атак.

Адаптація ML-моделей під специфіку мережі допоможе уникнути хибних спрацювань, що часто призводять до зниження продуктивності. Регулярне тестування та моніторинг нової інтеграції важливі для підтримки стабільної роботи системи та своєчасного виявлення будь-яких вразливостей у захисті.

Отже, інтеграція інтелектуальних функцій у протоколи маршрутизації не лише відповідає сучасним викликам у сфері кібербезпеки, а й створює проактивну систему захисту, здатну запобігати атакам ще до їх активного розгортання. Це забезпечить надійність, стабільність та безпеку корпоративних мереж у кіберпросторі.

Перелік використаних джерел.

1. Аль-Хорі, А. М., Сулейман, М. (2020). Огляд технік виявлення DDoS-атак. [Електронний ресурс]. - Режим доступу: https://www.researchgate.net/publication/341249972_A_Survey_on_DDoS_Attack_Detection_Techniques

2. Зуех, Дж. М., Ку, Х. (2019). Машинне навчання для виявлення мережевих вторгнень: огляд. [Електронний ресурс]. - Режим доступу: https://www.sciencedirect.com/science/article/pii/S1877050919301697

3. Дехгантана, М. В., Чу, К. К. Р. (2017). Машинне навчання для кібербезпеки: огляд. [Електронний ресурс]. - Режим доступу: https://link.springer.com/chapter/10.1007/978-3-319-57655-1_3