Терейковська Л.О., Можарівський О.В.

Національний авіаційний університет, Київ, Україна

Метод безпечної маршрутизації мережевого трафіку

Вступ. За останнє десятиріччя розвиток інформаційних та мережевих технологій дали змогу покращити якість сервісу, понизити вартість послуг, що сприятливо позначається на задоволенні потреб користувачів. Однак разом із настільки бурхливим розвитком технологій виникає все більше загроз на мережевому рівні.

Актуальність. Сьогодні часто постає питання про безпеку інформації в мережі. Кожного дня створюються нові атаки, що можуть призвести до порушення роботи мережі. А сучасні протоколи мережевої маршрутизації вразливі до атак, які можуть призвести до порушення цілісності, доступності, а також конфіденційності інформації, що передається в мережі. Вирішення цієї проблеми – створення методу безпечної маршрутизації.

Постановка задачі. При порушенні цілісності, доступності, конфіденційності потоку даних на мережевому рівні може відбутися витік конфіденційної інформації, що призведе до порушення роботи мережі та фінансових втрат організації. Потрібно розробити метод для мінімізації даних ризиків.

Мета. Аналіз вразливостей протоколів динамічної маршрутизації. Рекомендації щодо їх усунення.

Викладення матеріалу. Мережеві атаки можуть бути настільки ж різноманітними, як системи захисту проти них. Деякі атаки відрізняються великою складністю, а інші може реалізувати пересічний користувач, навіть не усвідомлюючи, до наслідків може може привести його діяльність. Для повного розуміння типів атак на мережеві ресурси необхідно знати обмеження, які були вкладені розробниками під час створення протоколу TCP/IP. Перші мережі створювалися для зв’язку між державними структурами, не підозрюючи можливий колосальний ріст цих мереж, та створення мережі Інтернет. Тому

ранні версії Інтернет-протоколу IP не мали ніяких функцій безпеки, через що були дуже вразливими для будь-яких типів атак. Однак з часом для протоколу IP почали розробляти нові реалізації доповнені різними мережевими процедурами, продуктами і послугами, що значно знижали ризики властиві для цього протоколу.

Для порушення процесу маршрутизації в мережі зловмиснику потрібно створити таку ситуацію:

- В мережі є шлях, що під контролем зловмисника, по якому проходить конфіденційна інформація ;
- В мережі відсутній шлях передачі пакетів між відправником та отримувачем, який би запезпечив достатню якість обслуговування;
- В мережі немає доступу до шляху передачі пакетів між відправником та отримувачем;

В сучасних мережах більшості атак порушення конфіденційності та цілісності інформації може уникнути шляхом використання сучасних криптографічних протоколів передачі інформації, наприклад: IPsec, PPTP, HTTPS, SSH і т.п. Однак, криптографічні протоколи захищають лише смислову складову даних потоку даних, але не факт їхньої передачі, хоча, наприклад, в військовій сфері, розголошення самого факту передачі інформації може стати критично небезпечним. Також криптографічні протоколи не дозволяють запобігти: атакам на порушення доступності інформації. Істотним недоліком перерахованих механізмів забезпечення інформаційної безпеки може бути також і те, що вони не враховують ризики порушення інформаційної безпеки. Представлені методи захисту працюють реактивно, відповідаючи на загрози, що виникають, проте не володіють превентивними заходами, які можуть дозволити попередження виникнення пагубних наслідків атаки.

Проаналізувавши сучасні механізми мережевої безпеки стало відомо, що в них не враховується ризик інформаційної безпеки, що не дає можливості їм працювати на упередження. Також стало відомо, що проблеми забезпечення

конфіденційності та цілісності інформації вирішуються за мережевих допомогою криптографічних протоколів, але вони не можуть забезпечити доступність інформації.

Керуючись висновками, які наведено вище, можна визначити що для створення методу безпечної маршрутизації необхідно:

- проведення досліджень з метою визначення ступеню впливу атак на доступність потоку даних при його передачі в мережах;
- вибір параметрів оцінки ризиків інформаційної безпеки;
- розробка методів оцінки ризиків інформаційної безпеки потоку даних в процесі маршрутизації в мережах;
- наведення рекомендацій щодо застосування ризиків інформаційної безпеки при виборі оптимального шляху передачі даних в мережах;

Список використаної літератури.

1. Aswal M.S. Threats and Vulnerabilities in Wireless Mesh Networks / M.S. Aswal, P. Rawat, T. Kumar // International Journal of Recent Trends in Engineering. – 2016. – Т. 2. – № 4. – С. 155-158.
2. У. Блэк «Интернет: протоколы безопасности. Учебный курс». – СПб: Питер, 2001. – 288с.:ил.
3. Кулаков Ю.А. Безопасная многопутевая маршрутизация в беспроводных сетях большой размерности / Ю.А. Кулаков, В.В. Лукашенко, А.В. Левчук // Захист інформації. – 2016. – Т. 13. – № 2(51). – С. 5-20.
4. Снегуров А.В. Метод формирования метрик маршрутизации, основанный на рисках информационной безопасности / А.В. Снегуров, В.Х. Чакрян // Системи управління, навігації та зв’язку – Вип. 4(24). – 2012. – С. 105-110.