АДАПТАЦИЯ ПОЛИТИКИ МАРШРУТИЗАЦИИ СЕТЕВОГО ТРАФИКА

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Игнатович Ю. Б., Игольник А. А.

Кункевич Д. П. – канд.техн.наук,доцент

Анализ сетевой безопасности показал, что традиционные методы обеспечения сетевой безопасности не всегда эффективно справляются с поставленными задачами. Одним из перспективных направлений развития средств и методов сетевой защиты является разработка систем сетевой безопасности на основе управления потоками трафика.

Развитие информационных технологий, а также их повсеместное проникновение в различные сферы деятельности привело к тому, что компьютерная информация имеет определенную стоимость. Поэтому одна из важнейших проблем развития информационных технологий – надежное обеспечение информационной безопасности.

По мере увеличения количества пользователей, получивших доступ к сети Интернет, а также развертывания компаниями своих сетей, задача обеспечения защиты становится более сложной и наиболее актуальной среди прочих задач сетевой безопасности.

Главной причиной, провоцирующей рост сетевой преступности, является несовершенство существующих средств и методов сетевой зашиты и неэффективность противодействия этих средств ряду информационных угроз. Подавляющее большинство нарушений в области информационной безопасности в сетях не могут контролироваться только средствами защиты на основе разграничения и контроля доступа (межсетевые экраны, фильтры, системы разграничения доступа и т.д.). Одним из перспективных подходов к построению сетевой защиты является адаптация политики динамической маршрутизации сетевого трафика к требованиям по информационной безопасности, который, в отличии от традиционных методов защиты, позволяет реализовать концепцию упреждающей защиты на основе управления потоками сетевого трафика. Сложность современных топологий распределенных сетей передачи данных не позволяет решать такие задачи методом простого перебора возможных вариантов решения. Поэтому, задача разработки методов и методик управления потоками сетевого трафика при помощи средств динамической маршрутизации является актуальной. Опасные воздействия на компьютерную информационную систему можно подразделить на случайные и преднамеренные. Анализ опыта проектирования, изготовления и эксплуатации информационных систем показывает, что информация подвергается различным случайным воздействиям на всех этапах цикла жизни системы и требования защиты необходимо соблюдать на всех уровнях сети.

Нарушителем могут быть люди самых разнообразных профессий, следовательно, и квалификация потенциального нарушителя, а также его техническая оснащенность, может быть различной.

Основными элементами политики в области сетевой безопасности являются идентификация и аутентификация пользователей. Идентификация требуется для предотвращения возможности несанкционированного доступа к ресурсам и данным. Аутентификация используется для проверки подлинности пользователя.

Для безопасности небольшой сети следует выполнять некоторые действия:

1. Использовать централизованной системы аутентификации и проверки подлинности;
2. Использование надежного антивирусного ПО;
3. Разделение прав доступа к ресурсам;
4. Внедрение криптографических средств для защиты информации.

Эти меры помогут серьезно повысить уровень безопасности сети и снизит вероятность утечки данных. Для максимального уровня защиты сети необходим комплексный подход с применением различных методов защиты информации.

Список использованных источников:

1. Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы: учеб. для вузов. — 3-е изд. — СПб.: Питер, 2006. — 958 с.

2. Столлингс В. Современные компьютерные сети. 2-е изд. — СПб.: Питер, 2003. — 783 с.

3. Труфанов А.И. Политика информационной безопасности вуза как предмет исследования // Проблемы Земной цивилизации. – Вып. 9. – Иркутск: ИрГТУ, 2004.

4. Крюков В.В., Майоров В.С., Шахгельдян К.И. Реализация корпоративной вычислительной сети вуза на базе технологии Active Directory // Тр. Всерос. науч. конф. «Научный сервис в сети Интернет». – Новороссийск, 2002