КОНФИДЕНЦИАЛЬНОСТЬ ПОТОКА ТРАФИКА

Теленков В.Д.

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

Латушко М.М. – канд. воен. наук

Аннотация. Указывается на сложность систем информационной безопасности, направленых на повышение защищенности информационно-телекоммуникационной сети по всем уровням эталонной модели взаимодействия открытых систем. Раскрываются недостатки и основные пути реализации услуги конфиденциальности потока трафика на физическом уровне передачи данных.

Высокие требования, предъявляемые к уровню защищенности информационно-телекоммуникационной сети, предопределяют необходимость проведения оценки эффективности функционирования систем защиты информации [1].

В настоящее время принято считать, что эффективность системы защиты информации определяется исключительно эффективностью средств защиты. На данный момент на рынке представлено большое разнообразие средств защиты информации, которые условно можно разделить на следующие группы [2]:

1. Средства разграничения доступа к информации в автоматизированных системах (паролирование);
2. Средства защиты информации при передаче ее по каналам связи (межсетевые экраны, криптомаршрутизаторы);
3. Средства защиты от информационного воздействия программ-вирусов (антивирусные системы и системы обнаружения вторжений).

Это означает, что ни одно отдельно выбранное средство защиты информации не может защитить информационно-телекоммуникационную сеть от комплекса целенаправленных воздействий компьютерных атак, а простая комбинация разнообразных средств защиты приводит к снижению эффективности защиты в целом из-за конфликтности параметров разнородных средств защиты. Поэтому в последнее время наметилась тенденция к построению сложных систем информационной безопасности, обеспечивающих защищенность информационно-телекоммуникационной сети по всем уровням эталонной модели взаимодействия открытых систем. В [1] определены основные услуги и механизмы защиты, их размещение по уровням эталонной модели взаимодействия открытых систем.

На физическом уровне передачи данных услугой защиты является конфиденциальность потока трафика. Конфиденциальность потока трафика означает обеспечение защищенности передаваемой информации таким образом, чтобы третьи лица не могли просматривать её содержимое. Это достигается использованием различных методов шифрования и протоколов. Например, при передаче банковских реквизитов через интернет-магазин используется протокол HTTPS, обеспечивающий шифрование данных между браузером покупателя и сервером магазина. Другой пример — использование виртуальных частных сетей (VPN). Ещё один пример — мессенджеры с поддержкой сквозного шифрования, такие как Telegram или Signal, где сообщения передаются в зашифрованном виде, и только отправитель и получатель имеют возможность их прочитать.

Недостатки обеспечения конфиденциальности потока трафика связаны главным образом с дополнительными сложностью и затратами ресурсов. Шифрование увеличивает нагрузку на устройства и каналы связи, снижает производительность и требует значительных вычислительных мощностей. Обеспечение конфиденциальности усложняет мониторинг и анализ сетевого трафика, поскольку зашифрованные пакеты невозможно проанализировать стандартными методами. Неправильная настройка или устаревшие стандарты шифрования создают риски утечки данных.

Для устранения указанных недостатков в обеспечении конфиденциальности потока трафика применяется следующие решения. Использование аппаратных ускорителей шифрования и современных энергоэффективных алгоритмов для снижения нагрузки на ресурсы. Применение решений глубокого анализа пакетов (DPI), позволяющее анализировать поведение зашифрованного трафика без дешифровки, повышая эффективность мониторинга. Регулярные аудиты и обновление программного обеспечения помогают минимизировать риск ошибок конфигурации и обеспечить высокий уровень защиты.

Список использованных источников:

1.Обеспечение устойчивости информационно-телекоммуникационных сетей в условиях информационного противоборства/ М.А. Коцыняк, А.И. Осадчий, М.М. Коцыняк, О.С. Лаута, В.Е. Дементьев, Д.Ю. Васюков – СПб.: ЛО ЦНИИС, 2014. – 126 с.

2. Раскин А.В., Пеляк В.С. К вопросу о сетевой войне // Военная мысль. 2005, № 3.