РАЗРАБОТКА ЗАЩИЩЁННОЙ КОРПОРАТИВНОЙ СЕТИ С ИСПОЛЬЗОВАНИЕМ ТЕХНОЛОГИИ ПРЕДОТВРАЩЕНИЯ ВТОРЖЕНИЙ

Д. В. Аникин

магистрант 2 курса факультета ФИКТ,
Национальный исследовательский университет ИТМО,
г. Санкт-Петербург, Россия

anikin406@gmail.com

Проблемы безопасности, с которыми сталкиваются современные специалисты по защите информации, невозможно устранить с помощью какого-либо одного приложения. Хотя повышение уровня безопасности оборудования, контроль доступа с помощью аутентификации, авторизации и учета, а также функции межсетевых экранов являются составными частями надлежащей сетевой защиты, этих возможностей все еще недостаточно, чтобы обезопасить сеть от стремительно распространяющихся через Интернет червей и вирусов. Сеть должна уметь мгновенно выявлять и нейтрализовать любые угрозы – от червей и вирусов.

Сдерживание вторжений всего лишь в нескольких точках сети больше не является приемлемым. Предотвращение вторжений требуется на всем протяжении сети для успешного определения и блокирования атак в каждой входящей и исходящей точке.

Необходимо пересмотреть парадигму сетевой архитектуры, чтобы обеспечить защиту от быстро распространяющихся и эволюционирующих атак. Сюда необходимо включить экономически эффективные системы для обнаружения и предотвращения угроз, такие как системы обнаружения вторжений (intrusion detection systems, IDS) или более масштабируемые системы предотвращения вторжений (intrusion prevention systems, IPS). Сетевая архитектура интегрирует эти решения во входные и выходные точки сети.

При реализации систем IDS или IPS необходимо досконально изучить типы доступных систем, локальные и сетевые подходы, способы размещения упомянутых систем, роли категорий сигнатур и возможные действия, которые сможет выполнять маршрутизатор в случае обнаружения атаки.

Ключевые слова: сеть; защита информации; сетевые атаки; система обнаружения вторжений (IDS); система предотвращения вторжений (IPS); программное обеспечение (ПО); базовая модель взаимодействия.

Интернет-черви и вирусы могут распространяться по всему миру в считанные минуты. Сеть должна мгновенно выявлять и нейтрализовывать любые угрозы – от червей и вирусов. Межсетевые экраны могут многое, но они не в состоянии защитить от вредоносного ПО и атак нулевого дня.

Атаки нулевого дня представляют собой компьютерную атаку, при которой используются уязвимости ПО, информация о которых неизвестна поставщику этого ПО или утаивается им. Термин «нулевой час» характеризует момент, когда обнаруживается вредоносный код, позволяющий использовать уязвимости ПО. В период времени, когда поставщик ПО занимается разработкой и распространением исправления, сеть остается уязвимой для вредоносного кода. Защита от таких быстро распространяющихся атак требует от специалистов в области сетевой безопасности перейти к более глубокому рассмотрению сетевой архитектуры. Сдерживание вторжений всего лишь в нескольких точках сети больше не является приемлемым.

Один из подходов к предотвращению попадания червей и вирусов в сеть заключается в том, чтобы специалисты постоянно выполняли мониторинг сети и анализировали файлы журналов, создаваемые сетевыми устройствами. Это решение не очень хорошо масштабируется. Анализ информации из журналов событий, выполняемый специалистами вручную, требует большого количества времени и не способен предоставить полный обзор атак, проводимых против сетевых инфраструктур. За время проведения анализа журналов атака может быть уже успешно завершена.

Реализация систем обнаружения вторжений предполагает пассивный мониторинг трафика в сети. Работая вне сети, это устройство сопоставляет поток трафика с известными вредоносными сигнатурами, подобно тому как выполняет проверку на наличие вирусов соответствующее ПО

Недостатком работы является то, что IDS не в состоянии остановить распространение вредоносных однопакетных атак к целевой системе до момента принятия мер против этих атак. Системам IDS зачастую требуется наличие вспомогательных сетевых устройств, таких как маршрутизаторы и межсетевые экраны, чтобы противодействовать атакам.

Самым существенным отличием между системами IDS и IPS является то, что IPS реагирует на угрозы незамедлительно и не допускает распространение вредоносного трафика, в то время как IDS пропускает такой трафик до принятия специальных мер.

Более оптимальным решением является устройство, которое может незамедлительно определять и предотвращать атаки. Такие функции выполняют системы предотвращения вторжений (IPS).

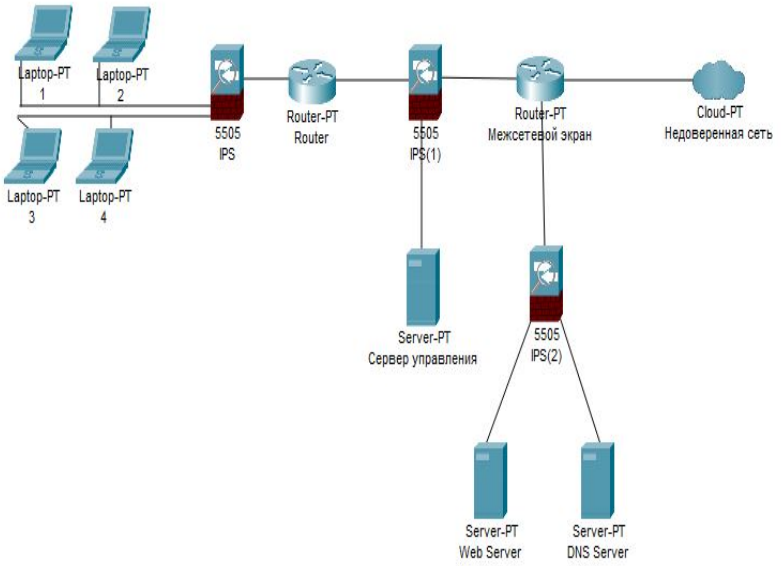
Обнаружение и остановка сетевых атак

Системы предотвращения вторжений (IPS) основаны на технологиях систем обнаружения вторжений (IDS). Однако устройства IPS реализуются во встроенном (inline) режиме. Это означает, что для обработки весь входящий и исходящий трафик должен проходить непосредственно через это устройство. IPS не допускает попадания пакетов в доверенную часть сети без выполнения их анализа. Это позволяет незамедлительно выявлять и принимать меры для решения сетевых проблем.

IPS выполняет мониторинг трафика на 3 и 4 уровне модели OSI. При этом выполняется анализ содержимого и полезной нагрузки пакетов для выявления более изощренных атак, проводимых с помощью вредоносных данных на уровнях со 2 по 7. На платформах IPS применяется комбинация технологий обнаружения, включая такие, которые основаны на сигнатурах и профилях, а также на методах обнаружения вторжений с помощью анализа протоколов. Такой более глубокий анализ позволяет IPS обнаруживать и блокировать атаки, которые проникают через традиционные устройства с функциями межсетевых экранов. Когда пакет поступает через интерфейс в IPS, то он не передается на исходящий или доверенный интерфейс, пока не будет проанализирован.

Защищённая корпоративная сеть с использованием сенсоров IPS представлена на рисунке 1.

Сетевая IPS может быть реализована с помощью выделенного или невыделенного IPS-устройства. Сенсоры определяют вредоносные и несанкционированные действия в режиме реального времени и при необходимости могут принять надлежащие действия. Сенсоры развертываются в определенных точках сети, что позволяет специалистам, обеспечивающим безопасность, отслеживать текущую сетевую активность, вне зависимости от места нахождения объекта атаки. Сетевые сенсоры IPS обычно настраиваются на выполнение анализа с целью предотвращения вторжений. В базовой операционной системе платформы, на которую устанавливается модуль IPS, ненужные сетевые службы отключаются, а для существенно важных обеспечивается защита.



Примечание – Источник: собственная разработка автора.

Рисунок 1 - **Защищённая корпоративная сеть с использованием сенсоров IPS**

Сетевые IPS предоставляют в реальном времени сотрудникам службы информационной безопасности исчерпывающую картину происходящего в сети, независимо от ее масштаба. Добавление новых хостов к защищенным сетям не требует дополнительных сенсоров. Дополнительные сенсоры необходимы, если превышены их номинальные возможности по пропускной способности трафика, когда их производительность не соответствует текущим требованиям или когда при проверке политики безопасности или проектировании сети нужно повысить защищенность на границах системы безопасности.

В ходе разработки защищённой корпоративной сети выяснилось, что предложенная система предотвращения вторжений способна с высокой вероятностью распознавать сетевые атаки, до того, как они попадут в корпоративную сеть. Сеть умеет мгновенно выявлять и нейтрализовывать любые угрозы. Система предотвращения вторжений предо-

ставляет в реальном времени отчёт происходящего в сети, независимо от ее масштаба, что гарантирует высокую степень её защищённости.

Важность данной разработки обуславливается актуальностью изученных тем. Дальнейшее исследование по этой теме поможет подтвердить гипотезу не только для защиты информации, но и для всех остальных видов деятельности IT сферы.

Библиографические ссылки

1. Middlemiss M., Dick G. Feature Selection of Intrusion detection data using a hybrid genetic of hybrid Intelligent systems. – IOSPress Amsterdam, 2003. – Pp. 519– 527.

2. KDD Cup 1999 Data [Электронный ресурс]. - Режим доступа : http://kdd.ics.uci.edu/databases/kddcup99. – Дата доступа : 13.02.2016.

3. Сергеев, Алексей Основы локальных компьютерных сетей / А. Сергеев. – М.: - Изд-во «Лань», 2020. - 184 с.

УЛУЧШЕНИЕ РЕЗУЛЬТАТОВ ВЫПОЛНЕНИЯ СТРАТЕГИЧЕСКОГО ПЛАНА ЗА СЧЕТ ВНЕДРЕНИЯ БИОМЕТРИЧЕСКОЙ ИДЕНТИФИКАЦИИ

Ю. В. Атрощенко

магистрант экономического факультета,
Белорусский государственный университет, г. Минск, Беларусь

yulia.atroshenko@yandex.by

Л. И. Стефанович

доктор экономических наук, профессор кафедры банковской экономики,
Белорусский государственный университет, г. Минск, Беларусь.

L.Stefanovich@tut.by

С момента увеличения объемов безналичных платежей, одной из первых задач кредитных организаций стало повышение защищенности сбережений клиентов. Благодаря развитию технологий актуальным следует считать использование биометрии в качестве механизма, обеспечивающего безопасность в том числе при осуществлении расчетов безналичным путем. В результате исследования была определена эффективность использования биометрической идентификации клиента в рамках тратегиского планирования деятельности банка.