УДК 004.728.4.056.53

КОМПЛЕКСНЫЙ ПОДХОД К ОБНАРУЖЕНИЮ СЕТЕВЫХ АТАК

Ульянов М.В. студент гр. ИТб-121, IV курс
Научный руководитель: А.В. Протодьяконов, к.т.н., доцент
Кузбасский Государственный Технический Университет
имени Т.Ф. Горбачева
г. Кемерово

Введение

Для минимизации рисков информационной безопасности в информационных корпоративных сетях в настоящее время актуальна разработка и внедрение систем обнаружения сетевых атак (СОА). Они представляют собой специализированные программные или программно-аппаратные средства, позволяющие осуществлять активный аудит и управление безопасностью (прогнозировать, обнаруживать, предупреждать, контролировать, реагировать в реальном масштабе времени на риски безопасности) в корпоративной сети. Решение задачи разработки эффективной защиты информации от сетевых атак требует разработки новых методов, способных противостоять распределенным сетевым атакам различного происхождения и более адекватно отображать сложную динамику случайных процессов этих атак. Требуется разработка методов выявления распределенных сетевых атак, использующих в комплексе современные методы поддержки принятия решений на основе теории интеллектуальных систем, позволяющих перейти при решении задач защиты продуктов и систем информационных технологий (СИТ) от принципа «обнаружение и ликвидация» к принципу «прогнозирование и предупреждение в реальном масштабе времени».

1. Обнаружение атак злоумышленного поведения

Принято выделять два базовых вида систем(3) обнаружения сетевых атак: работа первых заключается в поиске заранее известных признаков атаки; ко вторым относят программы, выявляющие аномалии в функционировании системы.

Если для обнаружения атаки требуется понимание ожидаемого поведения контролируемого нарушителя информации, то данная технология – технология обнаружения злоумышленного поведения. Работа систем обнаружения злоупотреблений базируется на составлении шаблонов, или «подписей» атак. Защитные системы этого типа эффективны на известных схемах атак, однако в случае новой неизвестной атаки или отклонения хода атаки от шаблона возникают серьезные проблемы. Поэтому приходится поддерживать большую базу данных, включающую каждую атаку и ее вариации, и непрерывно пополнять базы шаблонов. Также важно правильно определить объем выборки параметров, контролируемых методом обнаружения сетевой атаки, основанной на злоумышленном поведении. Малое их число или неправильно отобранные параметры могут привести к тому, что

модель описания поведения субъектов системы на основе данного метода будет неполной, и многие атаки не будут обнаружены. С другой стороны, слишком большое число параметров мониторинга, учитываемых методом, вызовет снижение производительности контролируемого узла за счет увеличенных требований к потребляемым ресурсам.

2. Обнаружение атак аномальной активности

Технология обнаружения сетевых атак, основанная на методах обнаружения аномальной (подозрительной) активности, в отличие от рассмотренной выше, более гибкая и позволяет обнаруживать неизвестные атаки. Системы обнаружения аномалий основаны на предположении, что все действия злоумышленника обязательно чем-то отличаются от поведения обычного пользователя, т. е. они аномальны.

Выявления атак, обусловленных аномальной активностью, основано на сравнении текущих значений параметров активности со значениями, которые на данный момент признаны нормальными. В качестве таких параметров могут выступать, например, количественные показатели использования системных ресурсов, интенсивности обращений к ресурсам или системным сервисам. Под текущими значениями параметров активности обычно понимаются средние значения, вычисленные на коротком интервале времени (от нескольких минут до нескольких часов), непосредственно предшествующем рассматриваемому моменту. Нормальными считаются средние значения этих параметров, вычисленные за достаточно большой период времени (от суток до нескольких месяцев).

Данная технология основана на выводе, что аномальное поведение субъекта (системы, программы, пользователя), проявляется как отклонение от нормального поведения. Примером аномального поведения может служить большое количество соединений за короткий промежуток времени, высокие загрузка центрального процессора и коэффициент сетевой нагрузки. Однако аномальное поведение не всегда является атакой. Например, атакой не является прием большого числа ответов на запрос об активности станций от системы сетевого управления.

Работе систем обнаружения аномальной активности предшествует период накопления информации, когда строится концепция нормальной активности системы, процесса или пользователя. Она становится эталоном, по которому оцениваются последующие данные. Поэтому при настройке и эксплуатации систем такой категории сталкиваются с двумя задачами:

– построением профиля субъекта (трудно формализуемой и трудоемкой задачей, требующей большой предварительной работы);

– определением граничных значений характеристик поведения субъекта для снижения вероятности появления одного из двух вышеназванных крайних случаев.

Эта технология требует постоянной регистрации всех действий контролируемого субъекта, необходимых для обнаружения аномальной активности, что существенно снижает производительность защищаемого хоста. Подобные системы сильно загружают центральный процессор, требуют больших объемов дискового пространства для хранения собираемых

данных и, в принципе, неприменимы для систем, критичных к быстродействию, работающих в режиме реального времени. Еще одним недостатком существующих систем обнаружения аномальной активности является то, что они созданы на основе предположений о стационарности сетевых процессов и взаимной независимости частных метрик, которые никогда не выполняются на практике. Это предопределяет использование в таких системах методов стационарной статистики, которые не пригодны для краткосрочного прогнозирования, что не позволяет реагировать на угрозу нарушения безопасности в реальном времени. Достаточно редкое обновление базы параметров нормального поведения позволяет нарушителям адаптировать своё поведение к требованиям системы обнаружения аномальной активности, которая в результате воспринимает его как законного пользователя. Игнорирование взаимной зависимости частных метрик приводит к неадекватной реакции системы, что выражается в большом числе ложных срабатываний.

3. Многоагентные системы обнаружения аномальной сетевой активности

Принимая во внимание текущие и перспективные тенденции развития систем информационных технологий, а также объективные недостатки описанных выше двух подходов к обнаружению сетевых атак, можно сделать вывод о необходимости смещения усилий на разработку и внедрение комплексных концепций построения систем защиты на основе распределенных вычислительных систем, с использованием механизмов защиты на основе активного аудита. Компоненты таких систем должны быть специализированы по типам решаемых задач, взаимодействовать друг с другом с целью обмена информацией и принятия согласованных решений, адаптироваться к реконфигурации аппаратного и программного обеспечения сети, изменению трафика, новым видам атак. Среди возможных технологий реализации такого подхода в качестве наиболее перспективного рассматривается технология интеллектуальных многоагентных систем.

Основные положения предлагаемого подхода состоят в следующем. Компоненты системы защиты информации (агенты защиты) представляют собой интеллектуальные автономные программы, реализующие определенные функции защиты с целью обеспечения требуемого класса защищенности. Они позволяют реализовать комплексную надстройку над механизмами безопасности используемых сетевых программных средств, операционных систем и приложений, повышая защищенность системы до требуемого уровня. Предполагается, что агенты распределены по хостам защищаемой компьютерной сети, специализированы по типам решаемых задач и взаимодействуют друг с другом с целью обмена информацией и принятия согласованных решений. Важно подчеркнуть, что в явном виде отсутствует «центр управления» семейством агентов – в зависимости от сложившейся ситуации ведущим может становиться любой из агентов, специализирующихся на задачах управления. В случае необходимости агенты могут клонироваться и прекращать свое функционирование. В зависимости от ситуации (вида и количества атак на компьютерную сеть, наличия вычислительных ресурсов для

выполнения функций защиты) может генерироваться несколько экземпляров агентов каждого класса. Они адаптируются к реконфигурации сети, изменению трафика и новым видам атак, используя накопленный опыт.

Предлагаемый подход на основе технологии интеллектуальных многоагентных систем позволит использовать в СОА следующие принципиально новые подходы, существенно повышающие эффективность системы защиты от распределенных сетевых атак:

- мобильность, система построена на мобильных агентах, что позволяет сделать систему гибкой, легко реконфигурируемой, жизнестойкой;
- активность, система не только фиксирует факты удаленных сетевых атак, но и проводит активные мероприятия против удаленного злоумышленника;
- самоорганизация, использование принципов и упрощенной структуры иммунно системы человека, позволяет решить задачи восстановления системы в результате сбоев, самоконтроля для обнаружения собственных ошибок;
- специализация по типам решаемых задач;
- адаптация к реконфигурации аппаратного и программного обеспечения сети, изменению трафика, новым видам атак;
- осуществление поддержки принятия наиболее рационального решения по блокированию распределенной во времени и пространстве сетевой атаки.

Осуществление процесса прогнозирования и обнаружения распределенных сетевых атак является основным содержанием специфических функций многоагентной системы обнаружения сетевых атак.

Заключение

Обнаружение сетевых атак на ресурсы СИТ весьма сложный технологический процесс, который связан со сбором больших объемов информации о функционировании СИТ, анализом этих данных и, наконец, выявлением факта атаки. Для эффективного прогнозирования и обнаружения атак требуется комплексное применение различных сигнатурных методов и методов обнаружения аномальной сетевой активности.

Поскольку решение проблемы повышения эффективности защиты информации в корпоративных сетях видится в использовании адаптивных методов, позволяющих в реальном масштабе времени осуществлять обнаружение нестационарных процессов, характеризующих сетевые атаки, то целесообразно рассмотреть подход, объединяющий в себе метод многоагентных систем с методами адекватного выявления признаков атак на основе статистических методов теории вероятностей, нечетких вероятностно-статистических методов, методов теории интеллектуальных систем, а также методов искусственных нейронных сетей. Эти методы при их согласованной реализации в СОА должны позволять в широком диапазоне условий функционирования корпоративных сетей и СИТ адекватно в реальном масштабе времени обнаруживать нестационарные случайные динамические процессы аномальной активности и злоумышленного поведения в сети и СИТ при малых вероятностях ложных тревог и пропуска сетевых атак

1. Гамаюнов Д. Ю., Смелянский Р. Л., Модель поведения сетевых объектов в распределенных вычислительных системах. - 2007 с. 20-31.

2. Лукацкий А.В. Обнаружение атак. – СПб: БХВ-Петербург, 2003. – 596 с.

3. Щеглов А.Ю. Защита компьютерной информации от несанкционированного доступа. – СПб. 2004. – 38