УДК 004.031.43

МНОГОКОМПОНЕНТНЫЕ СИСТЕМЫ ОБНАРУЖЕНИЯ СЕТЕВЫХ АТАК

П.А. ЖУРАВКОВ
(Представлено: Е.Р. СУХАРЕВ)

Рассматривается подход к построению многокомпонентных систем обнаружения сетевых атак. Анализируются два базовых вида систем обнаружения атак: система поиска по паттернам и система, выявляющая аномалии в функционировании системы.

В настоящее время актуальна разработка и внедрение систем обнаружения сетевых атак для минимизации рисков информационной безопасности в информационных корпоративных сетях. Данные системы представляют собой специализированные программные или программно-аппаратные средства, которые позволяют вести активный аудит и управление безопасностью (прогнозировать, обнаруживать, предупреждать, контролировать, реагировать в режиме реального 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.

Обнаружение атак злоумышленного поведения. Выделяются два базовых вида систем обнаружения сетевых атак: системы поиска заранее известных признаков атаки и системы, выявляющие аномалии в функционировании системы.

Если для обнаружения атаки требуется понимание ожидаемого поведения контролируемого нарушителя информации, то это технология обнаружения злоумышленного поведения. Работа систем обнаружения злоупотреблений базируется на создании шаблонов атак. Защитные системы такого типа эффективно показывают себя на известных схемах атак, однако в случае новой, ранее неизученной атаки или отклонения хода атаки от шаблона возникают проблемы [1]. Поэтому приходится постоянно поддерживать базу данных, включающую сигнатуру каждой атаки и ее вариации, непрерывно пополнять базы шаблонов. Немаловажным является правильно определить выборку параметров, контролируемых методом обнаружения сетевой атаки, основанной на злоумышленном поведении. Их малое количество или неправильно выбранные параметры могут привести к неполноте модели описания поведения атак, поэтому многие атаки могут быть не обнаружены [2]. С другой стороны, если взять слишком много параметров, учитываемых методом, это вызовет снижение производительности наблюдаемого узла за счет увеличения вычислительных операций.

Обнаружение атак аномальной активности. Метод обнаружения сетевых атак, основанный на методах обнаружения аномальной (подозрительной) активности, в отличие от рассмотренной выше, более гибок 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 с нормальными значениями [3]. В качестве таких параметров могут выступать, например, количественные показатели использования системных ресурсов, интенсивности обращений к ресурсам или системным сервисам. Текущими значениями параметров активности являются средние значения, которые вычислены за короткий промежуток времени (от нескольких секунд до нескольких минут). Нормальными считаются средние значения этих параметров, вычисленные за большой период времени, относительно текущих значений параметров (от суток до нескольких недель).

Данный метод основан на том, что аномальное поведение субъекта проявляется как превышение нормального поведения. В частности, аномальным поведением может быть большое количество соединений за короткий промежуток времени. Однако аномальное поведение не всегда является атакой. Например, увеличение активности пользования социальными сервисами в момент празднования какого-либо мероприятия не является атакой.

Перед тем как система сможет начать работать, ей необходим период накопления информации, когда создается профиль нормальной активности системы, процесса или пользователя. Он становится эталоном, по которому оцениваются последующие данные.

Эта технология требует постоянной регистрации всех действий контролируемого субъекта, необходимых для обнаружения аномальной активности, что ведет к существенному снижению производительности защищаемого узла. Подобные системы сильно загружают центральный процессор, требуют больших объемов дискового пространства для хранения собираемых данных и в принципе не могут применяться в системах, которые работают в режиме реального времени, то есть систем критичных к быстродействию [4].

Многокомпонентные 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 [5]. 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 многокомпонентных систем.

Основные положения предлагаемого подхода состоят в следующем. Компоненты системы защиты информации (агенты защиты) представляют собой автономные программы, реализующие определенные функции защиты для обеспечения требуемого уровня 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 всем узлам защищаемой информационной системы и способны собирать и обрабатывать собранную информацию независимо от остальных агентов, работающих на других узлах. Они должны адаптироваться к реконфигурации сети, то есть изменению топологии сети в информационной системе, либо установке или удалению сетевых устройств на узлах. Очевидно, что собирать и анализировать данные агенты должны постоянно. Предлагаемый подход на основе многокомпонентных систем позволит использовать новые подходы, повышающие эффективность системы обнаружения сетевых аномалий, такие как мобильность (сбор и обработка сетевых данных построены на мобильных агентах, что позволяет сделать систему гибкой), адаптация к реконфигурированию аппаратного и программного обеспечения системы или изменению трафика, активность (система не только фиксирует факты удаленных сетевых атак, но и проводит действия направленные на оповещение специалистов информационной безопасности).

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

ЛИТЕРАТУРА

1. Основы информационной безопасности : учеб. пособие для вузов / Е.Б. Белов [и др.]. – М. : Горячая линия – Телеком, 2006. – 544 с.
2. Щеглов, А.Ю. Защита компьютерной информации от несанкционированного доступа / А.Ю. Щеглов. – СПб. : Наука и техника, 2004. – 384 с.
3. Мониторинг состояния автоматизированной системы и обеспечение стабильности / А.А. Сапожников [и др.]. // Информационно-телекоммуникационые системы : сб. материалов Всерос. конкурса инновационных проектов аспирантов и студентов по приоритетному направлению развития науки и техники. – М. : ГНИИ ИТТ «Информика», 2005. – С. 123–124.
4. Сапожников, А.А. Практика централизованного мониторинга сетей / А.А. Сапожников // Проблемы функционирования информационных сетей : материалы междунар. конф. – Новосибирск : ЗАО РИЦ Прайс Курьер, 2006. – С. 257–260.
5. Сапожников, А.А. Обнаружение аномальной сетевой активности / А.А. Сапожников // Докл. Томского гос. ун-та систем управления и радиоэлектроники. – 2009. – № 1. – С. 79–80.
6. Емельянова, Ю.Г. Современный уровень и тенденции развития средств обеспечения сетевой безопасности систем облачных вычислений / Ю.Г. Емельянова, Э. Мбайкоджи, И.В. Соченков // Вестн. Рос. ун-та дружбы народов. Серия Математика. Информатика. Физика. – М. : РУДН, 2012. – № 2. – С. 116–126.
7. Шипулин, А. Мониторинг аномалий сетевой активности в промышленных система / А. Шипулин // Безопасность деловой информации. – 2015. – С. 32.
8. Aydin, M. A hybrid intrusion detection system for computer netwrok security Text / M. Ali Aydin, A. Halim Zaim, K. Gokhan Ceylan // Computer & Electrical Engineering. – 2009. – Vol. 35, Iss. 3, May. – P. 517–526.
9. Performance Measurement and Analysis of H. 323 Traffic Text / P. Calyam [et al.] // Passive and Active Network Measurement. – 2004. – P. 137–146.
10. Garfinkel, S. Practical Unix & Internet Security, O'Reilly / S. Garfinkel, A. Schwartz, G. Spafford, 2003. – 984 p.
11. Hoglund, G. Exploiting Software. How to Break Code / G. Hoglund, G. McGraw, A. Wesley, 2004. – 512 p.
12. Levenberg, K. A Method for the Solution of Certain Problems in Least Squares / G. Hoglund // Quart. Appl. Math. – 1944. – Vol. 2. – P. 164–168.
13. Sperotto, A. Anomaly characterization in flow-based traffic time series Text / A. Sperotto, R. Sadre, A. Pras // Proceedings of the 8th IEEE International Workshop on IP Operations and Management, IPOM 2008, Samos, Greece, 2008.