СЕТЕВАЯ МОДЕЛЬ АКТИВНОГО МОНИТОРИНГА РАБОЧИХ СТАНЦИЙ РАСПРЕДЕЛЕННОЙ ИНФОРМАЦИОННО-ВЫЧИСЛИТЕЛЬНОЙ СЕТИ

А.А. Цветков
Россия, г. Шуя

С развитием сетевой инфраструктуры, с увеличением количества пользователей сети и объема распределенных информационных ресурсов проблема обеспечения информационной безопасности образовательных учреждений приобретает все большую сложность. В последнее время ситуация осложняется тем, что сбой в системе безопасности и утечка информации могут быть произведены особым персонажем, называемым инсайдером – это конкретный человек, сотрудник организации, имеющий доступ к информации, недоступной широкой публике.

Общепринято, что даже самые надежные методы защиты не гарантируют абсолютной безопасности, поэтому чтобы пресечь попытки несанкционированного проникновения в систему, рекомендуется регулярно контролировать операции клиентов корпоративной сети, поскольку согласно статистике наибольший ущерб системе наносят не внешние, а внутренние угрозы [1].

Наличие инсайдеров в качестве пользователей распределенной вычислительной сети приводит к недостаточной информированности администратора сети о состоянии информационной безопасности системы. То есть для обеспечения устойчивости функционирования информационно-вычислительной сети необходимо своевременно получать актуальную информацию о состоянии сетевых ресурсов и несанкционированных действиях пользователей с целью дальнейшей идентификации профиля пользователя и по возможности выявления инсайдеров сети.

Таким образом, в интересах идентификации профиля пользователя и разграничения прав доступа необходима разработка концептуальной модели активного мониторинга рабочих станций распределенной информационно-вычислительной сети.

В общем случае под мониторингом понимается процесс наблюдения и регистрации данных о каком-либо объекте, хранения и анализа небольшого количества ключевых (явных или косвенных) признаков/параметров описания данного объекта для вынесения суждения о поведении/состоянии данного объекта в целом. То есть цель мониторинга – вынесение суждения об объекте в целом на основании анализа небольшого количества характеризующих его признаков. Применительно к компьютерной сети наблюдаемым объектом при мониторинге является сама сеть, в результате выносится суждение о ее состоянии. Термином мониторинг рабочих станций сети назовем работу системы, которая выполняет постоянное прямое или косвенное наблюдение за действиями пользователей в поисках попытки нарушений прав доступа, а также с целью сбора информации о поведении пользователей в сети.

Существует два типа мониторинга: активный и пассивный. Активный мониторинг подразумевает опрос устройств с определенной периодичностью с целью определения доступности самих устройств и сервисов, которые они предоставляют, проверки текущего состояния устройств, а также посредством специализированных программных средств сбора информации о работе пользователей в сети. Пассивный мониторинг подразумевает ожидание от устройств сообщений о событиях, происходящих в системе [2]. Вызывает интерес главным образом режим активного мониторинга, поскольку само устройство не всегда способно обнаружить возникающие сбои, кроме того, активный мониторинг может проводиться централизованно, решая определенные задачи во всей сети, а не только по отношению к отдельным устройствам. В частности сбор информации о действиях пользователях в сети требует именно активного мониторинга.

То есть активному мониторингу должны подвергаться пользовательские права доступа к информационным ресурсам для выявления случаев попытки доступа к ресурсам клиентов с заведомо недостаточными на то правами, когда они вдруг приобретают сверхбольшие права. Все это позволит предотвратить несанкционированные действия пользователей, повысить корпоративную безопасность.

Прежде чем приступать к конфигурированию системы мониторинга, необходимо изучить строение сети и определить оптимальное расположение инструментов мониторинга, которые могут находиться на одном или нескольких серверах или на рабочей станции администратора. Как правило, мониторинг требуется круглосуточный, поэтому устанавливать систему мониторинга надо на серверах, которые работают в круглосуточном режиме. При выборе местоположения сервера необходимо руководствоваться двумя критериями: минимальной удаленностью сервера от основных устройств, мониторинг которых необходимо производить, и емкостью Интернет-канала между сервером мониторинга и станциями с клиентами, которые будут к нему подключаться [2].

В последнее время практически стандартом построения информационных систем стала «клиент-серверная» модель взаимодействия компьютеров в сети, состоящая из нескольких неравноправных звеньев, на которых размещены отдельные компоненты приложения с целью их более эффективного функционирования. При этом каждое звено играет свою роль – сервер владеет информационными ресурсами, а клиент имеет возможность обращаться к этим ресурсам.

Кроме того, наблюдается тенденция к большему использованию модели распределенного приложения. Особенностью таких приложений является логическое разделение приложения на несколько частей, каждая из которых может выполняться на отдельном компьютере. Выделенные части приложения взаимодействуют друг с другом, обмениваясь сообщениями в заранее согласованном формате.

На современном этапе модель клиент-серверной архитектуры актуальна и широко используема в большом количестве организаций, когда в рамках головного подразделения устанавливается сервер, обрабатывающий поступающие запросы пользователей, а к нему локально подключаются различные клиенты. Работу сети обеспечивают системные и сетевые администраторы, которые имеют доступ к серверу, настраивая все необходимые функции и конфигурацию сервера, они также назначают права доступа пользователям к определенным типам и местам хранения данных, назначают определенные правила для рабочих групп пользователей, достигая при этом безопасности и сохранности коммерчески важных данных. Отметим, что дополнительной возможностью обеспечения безопасности и доступности данных является размещение основной базы данных на другом электронном устройстве, являющимся также частью сети.

В общем случае, архитектура клиент-сервер наиболее оправдывает себя при построении локальной или распределенной сети, в которой имеется отдельный сервер и электронные узлы (клиенты). Вычислительная сетевая нагрузка разделяется между узлами, обеспечивая при этом их корректную совместную работу.

Таким образом, сетевая модель активного мониторинга рабочих станций может быть представлена в следующем виде. Все компьютеры локальной сети организации объединены в домен. В сети могут присутствовать различные сервера, такие как прокси-сервер, файловый сервер, сервер баз данных, сервер Backup, контроллер домена, сервер администрирования антивирусов и другие. Прокси-сервер предназначен для управляемого доступа в Интернет посредством политик межсетевого экрана, помимо того он предоставляет возможность мониторинга Интернет-трафика. Файловый сервер хранит файлы общего пользования. Сервер баз данных предоставляет доступ к базам данных организации. Сервер Backup производит резервное копирование важной информации, определенной администратором сети. Контроллер домена обеспечивает централизованную авторизацию пользователей. Сервер

администрирования антивирусов удаленно и централизованно управляет работой программ-антивирусов, установленных на компьютерах вычислительной сети.

В сети присутствуют рабочие станции, при этом каждый пользователь должен входить в систему под своей доменной учетной записью, которая определяет для него права доступа к сетевым и Интернет-ресурсам.

Для централизованного сбора и обработки информации о действиях пользователей в сети целесообразно установить сервер мониторинга. Он ведет активный мониторинг посредством анализа логов аудита файловых систем и сетевого трафика. Так, с прокси-сервера считывается лог сетевой активности пользователей, содержащий в себе сведения об успешных и неуспешных попытках доступа к Интернет-ресурсам. С контроллера домена может быть получена информация о неудачных попытках авторизации, о сессиях пользователей и т.п. Файловый сервер и сервер баз данных предоставляют логи аудита доступа к файлам и папкам. Однако нередки случаи, когда от имени пользователей действия производит вредоносное программное обеспечение, поэтому также необходимо отслеживать вирусную активность. Отчеты об обнаруженных угрозах в сети могут быть считаны с сервера администрирования антивирусов.

Анализ собранных отчетов в совокупности позволит идентифицировать профиль пользователя, выявить аномальную сетевую активность с целью проведения более детального разграничения прав доступа, что в свою очередь приведет к повышению уровня безопасности распределенной информационно-вычислительной сети.

Литература

1. Защита информации в архитектурах клиент/сервер [Электронный ресурс]. URL: http://www.infocity.kiev.ua/hack/content/hack054.phtml (дата обращения: 15.04.2013).

2. The Dude. Практический мониторинг (Часть 1) [Электронный ресурс]. URL: http://habrahabr.ru/post/145923 (дата обращения: 15.04.2013).