ЗАЩИТА ИНФОРМАЦИОННЫХ СИСТЕМ ОТ ПОТЕНЦИАЛЬНОЙ УГРОЗЫ «ПЯТОЙ КОЛОННЫ»

В.А. Сердюк
ЗАО «РНТ»

В последние годы частота несанкционированных воздействий на информационные системы (ИС) постоянно увеличивается, что неминуемо приводит к огромным финансовым и материальным потерям. Подтверждением этому являются данные ежегодных исследований Института компьютерной безопасности США, которые показывают, что в 2003 году, например, количество успешных вторжений в ИС в сравнении с предыдущим годом возросло в несколько раз. При этом засвидетельствован весьма интересный факт, говорящий о том, что более половины всех нарушений совершают работники компаний, то есть внутренние пользователи ИС. Это наводит на мысль о том, что имеет место формирование весьма опасной «пятой колонны», результаты действий которой могут привести к катастрофическим последствиям для владельцев ИС.

Известно, что в последние несколько лет защита ИС от внутренних нарушителей обеспечивается преимущественно специализированными средствами разграничения доступа пользователей к информационным ресурсам. При помощи этих средств каждому пользователю назначаются определенные права, в соответствии с которыми ему разрешается (или запрещается) локальный доступ к информации, хранящейся в его компьютере, или же удаленный доступ по каналам связи к информации, имеющейся на других компьютерах.

И все же приходится констатировать, что этот подход не решает всей проблемы защиты информационных ресурсов от злоумышленников, действующих изнутри ИС. Связано это с двумя основными факторами:

1. Средства разграничения локального доступа не имеют возможности обеспечить защиту от авторизованных пользователей, пытающихся выполнить несанкционированные действия. Так, пользователь может непреднамеренно установить и запустить на своей рабочей станции вредоносное программное обеспечение (информационные вирусы, программы типа «Троянский конь» и др.). Другим примером несанкционированных действий, защита от которых не может быть обеспечена средствами разграничения доступа, является запись на внешние носители или вывод на печать конфиденциальной информации, к которой пользователь легально получил доступ. Для выявления таких действий на ранней стадии следует применять системы активного мониторинга рабочих станций локально-вычислительной сети (ЛВС).

2. Средства разграничения удаленного доступа не обеспечивают защиту от сетевых атак, которые могут быть проведены внутренними пользователями системы. Такие атаки базируются на уязвимостях, которые могут присутствовать в программно-аппаратном обеспечении серверов и рабочих станций ИС. Примерами уязвимостей являются нестойкие пароли, некорректные настройки программного обеспечения (ПО), ошибки в прикладном ПО и т.д. Успешное проведение сетевых атак может привести к нарушению конфиденциальности, целостности или доступности информации в системе. Для своевременного обнаружения и блокирования таких атак необходимо использовать средства обнаружения, известные как IDS-системы (Intrusion Detection Systems).

Таким образом, обеспечение эффективной защиты от внутренних нарушителей информационной безопасности требует использования дополнительных средств защиты, таких как системы активного мониторинга рабочих станций (САМ), а также системы обнаружения атак (СОА). Рассмотрим эти типы средств защиты более подробно.

СИСТЕМЫ ОБНАРУЖЕНИЯ АТАК

СОА предназначены для выявления и противодействия сетевым атакам злоумышленников. Системы представляют собой специализированное программно-аппаратное обеспечение с типовой архитектурой, включающей в себя следующие компоненты (рис. 1):

- модули-датчики для сбора необходимой информации о сетевом трафике ИС;
- модуль выявления атак, выполняющий обработку данных, собранных датчиками, с целью обнаружения информационных атак;
- модуль реагирования на обнаруженные атаки;
- модуль хранения конфигурационной информации, а также информации об обнаруженных атаках. Таким модулем, как правило, выступает стандартная СУБД, например, MS SQL Server, Oracle или DB2;
- модуль управления компонентами СОА.

В составе СОА могут быть использованы два типа датчиков — сетевые и хостовые. Сетевые датчики предназначены для сбора информации о пакетах данных, передаваемых в том сегменте ИС, где установлен датчик. Хостовые же датчики устанавливаются на серверы ИС и предназначены для сбора информации о пакетах данных, ко-

Рис. 1. Типовая архитектура систем обнаружения атак

торые поступают на сервер с датчиком.

Информация, собранная сетевыми и хостовыми датчиками, анализируется СОА с целью выявления возможных атак нарушителей. Анализ данных может проводиться при помощи двух основных групп методов — сигнатурных и поведенческих.

Сигнатурные методы описывают каждую атаку в виде специальной модели или сигнатуры. В качестве последней могут выступать: строка символов, семантическое выражение на специальном языке, формальная математическая модель и т. д. Алгоритм работы сигнатурного метода заключается в поиске сигнатур атак в исходных данных, собранных сетевыми и хостовыми датчиками СОА. При обнаружении искомой сигнатуры СОА фиксирует факт соответствующей информационной атаки. Преимуществом этих методов является их высокая точность работы, а очевидным недостатком — невозможность обнаружения тех атак, сигнатуры которых не определены при помощи методов.

Поведенческие методы, в отличие от сигнатурных, базируются не на моделях информационных атак, а на моделях штатного процесса функционирования ИС. Принцип работы поведенческих методов заключается в обнаружении несоответствия между текущим режимом функционирования ИС и моделью штатного режима работы, заложенной в параметрах метода. Любое такое несоответствие рассматривается как информационная атака. Преимуществом методов данного типа является возможность обнаружения новых атак без необходимости постоянного изменения параметров функционирования модуля. Недостатком же этой группы методов является сложность создания точной модели штатного режима функционирования ИС.

После выявления в информационной системе атаки СОА имеет возможность предпринять ответные действия, направленные на ее блокирование. За реализацию этих действий отвечает модуль реагирования СОА.

Реагирование СОА может осуществляться активным и пассивным способами. К пассивным методам реагирования относится простое оповещение администратора СОА о выявленных атаках. К активным же можно отнести следующие методы:

- блокирование TCP-соединения, по которому была реализована атака. Такое закрытие реализуется путем посылки субъектам соединения специального TCP-сегмента с установленным флагом RST;
- запуск заданной внешней программы с определенными параметрами. Наличие такой функции модуля реагирования позволяет администратору СОА дополнять существующие методы реагирования своими собственными методами, реализованными в виде внешних подпрограмм;
- реконфигурация межсетевого экрана (МЭ) с целью блокирования трафика, поступающего от хоста нарушителя. В настоящее время большая часть МЭ имеет соответствующие внешние интерфейсы, обеспечивающие взаимодействие МЭ с СОА. Примером такого интерфейса является интерфейс OPSEC для МЭ Check-Point FW-1.

Учитывая тот факт, что СОА могут сами выступать в роли объектов атаки злоумышленников, эти системы обязательно должны быть оснащены подсистемой собственной безопасности.

Характерными примерами коммерческих СОА являются системы «Форпост», «RealSecure» и «NetProwler».

Однако необходимо отметить, что только использование СОА не позволяет полностью решить проблему защиты от несанкционированных действий внутренних пользователей ИС. В первую очередь это связано с тем, что СОА обнаруживают лишь те информационные атаки, которые можно выявить посредством анализа только пакетов данных, циркулирующих в ИС. Данный факт не позволяет СОА выявлять те несанкционированные действия пользователей, которые никак не связаны с сетевым трафиком ИС. Как уже отмечалось выше, для выявления и блокирования таких действий необходимо использовать системы активного мониторинга, описание которых приводится ниже.

СИСТЕМЫ АКТИВНОГО МОНИТОРИНГА РАБОЧИХ СТАНЦИЙ ИС

Системы активного мониторинга рабочих станций ИС (САМ), так же как и СОА, предназначены для выявления и блокирования информационных атак, но не на уровне сети, а на уровне рабочих станций ИС. Архитектура систем активного мониторинга аналогична структуре СОА, отображенной на рис. 1. Датчики САМ устанавливаются на рабочие станции пользователей ИС и позволяют собирать информацию обо всех событиях, происходящих на них.

Это может быть информация:

- о приложениях, запускаемых на рабочих станциях;
- о пользователях, работающих на станции в текущий момент времени;
- о файловом доступе приложений;
- о сетевом трафике, который формируется приложениями ИС и др.

Собранная информация поступает в модуль анализа данных САМ, где осуществляется ее обработка. Предварительно администратор безопасности должен выполнить настройку модуля анализа САМ, то есть определить требования, которые разрешают или запрещают пользователям ИС выполнение оп-

ределенных операций на рабочих станциях. Совокупность таких требований представляет собой политику безопасности САМ, которая может являться частью общей политики безопасности организации. Так, в соответствии с заданной политикой безопасности некоторым пользователям может быть запрещена работа с принтерами или доступ к определенным файлам. Любое событие, зафиксированное датчиками САМ и нарушающее ранее заданную политику, считается информационной атакой.

Политика безопасности САМ может включать в себя разные группы требований, которые формируются на основе двух базовых принципов:

- «всё, что не запрещено,— разрешено». Политика безопасности САМ, построенная на основе этого принципа, явно определяет те действия пользователей, выполнение которых запрещено. При этом все остальные действия, выполняемые пользователями, считаются разрешенными. Для выявления нарушений такой политики используются сигнатурные методы анализа;
- «всё, что не разрешено,— запрещено». Политика безопасности САМ, построенная на основе этого принципа, явно определяет только разрешенные действия пользователей. Все остальные действия согласно этой политике являются нарушениями, для обнаружения которых используются поведенческие методы анализа.

В случае выявления нарушений политики безопасности САМ может реализовывать пассивные и активные методы реагирования. К пассивным методам относится оповещение администратора безопасности об обнаруженных несанкционированных действиях пользователей. Такое оповещение может осуществляться путем отображения соответствующего сообщения на консоли администратора или отправки сообщения по электронной почте. Активные методы подразумевают блокирование тех действий пользователей, которые нарушают заданную политику безопасности. Так же как и СОА, системы активного мониторинга могут сочетать активные и пассивные методы реагирования.

САМ должны быть также оснащены подсистемой собственной безопасности, позволяющей защитить компоненты системы от несанкционированных воздействий нарушителей.

Примерами коммерческих реализаций САМ являются системы «Урядник/Enterprise Guard», «StatWin» и «NetIntelligence».

Рассмотрим более подробно функциональные возможности САМ на примере системы управления политикой безопасности «Урядник/Enterprise Guard», разработанной отечественной компанией «IDS-Technology».

СИСТЕМА УПРАВЛЕНИЯ ПОЛИТИКОЙ БЕЗОПАСНОСТИ «УРЯДНИК/ENTERPRISE GUARD»

САМ «Урядник/Enterprise Guard» предназначена для выполнения следующих функций:

- выявления и блокирования действий пользователей, нарушающих заданную политику безопасности ИС;
- мониторинга и контроля работы персонала ИС;
- сбора доказательств, необходимых для расследования инцидентов, связанных с нарушением информационной безопасности ИС;
- мониторинга работы приложений, запущенных на рабочих станциях пользователей.

Система имеет распределенную архитектуру и включает в себя следующие компоненты (рис. 2):

- *программные агенты*, устанавливаемые на рабочие станции пользователей ИС и предназначенные для сбора информации о контролируемых событиях. При этом программные агенты используют для своей работы минимальный объем программно-аппаратных ресурсов и не влияют на производительность рабочих станций пользователей;
- *сервер системы*, основная задача которого заключается в сборе, хранении и анализе информации, поступающей от агентов системы;
- *консоль администратора*, предназначенная для централизованного управления сервером и агентами системы, а также для отображения результатов ее работы. Консоль администратора также включает в себя специальный редактор, при помощи которого задается политика безопасности;
- *генератор отчетов*, представляющий собой отдельный программный модуль, предназначенный для формирования отчетов на основе результатов работы системы.

Агенты системы управления политикой безопасности «Урядник/Enterprise Guard» позволяют осуществлять сбор информации о следующих событиях на рабочих станциях пользователей ИС:

- начало / завершение сеанса работы;
- запуск / остановка приложений;
- файловые операции запущенных приложений;
- изменение контрольных сумм приложений;
- открытие диалоговых окон в рамках приложений;
- клавиатурный ввод пользователей ИС;
- доступ приложений к ресурсам Интернет;
- печать документов из приложений;
- отправка/получение электронных почтовых сообщений.

На основе анализа информации,

Рис. 2. Структура системы управления политикой безопасности «Урядник/Enterprise Guard»

собираемой агентами, САМ «Урядник/Enterprise Guard» позволяет выявлять те события, которые нарушают политику безопасности, заданную администратором системы. В случае выявления таких событий предусмотрены следующие методы реагирования:

- оповещение администратора о выявленном нарушении политики безопасности путем вывода сообщения на консоль или отсылки его по электронной почте;
- блокирование рабочей станции пользователя, нарушившего политику безопасности;
- генерация снимка рабочей области станции пользователя, нарушившего политику безопасности;
- блокирование работы приложения, нарушившего политику безопасности;
- вывод предупреждающего информационного сообщения пользователю, нарушившему политику безопасности.

САМ «Урядник/Enterprise Guard» оснащена подсистемой собственной безопасности, обеспечивающей целостность программного обеспечения системы, а также криптографическую защиту служебной информации, передаваемой между компонентами системы по каналам связи. Дополнительно система имеет встроенные механизмы контроля «живучести» собственных компонентов, которые базируются на процедурах проверки работоспособности агентов, установленных на рабочих станциях пользователей.

В отличие от зарубежных аналогов система «Урядник/Enterprise Guard» имеет сертификат Гостехкомиссии России.

Системы активного мониторинга, такие как «Урядник/Enterprise Guard», могут использоваться в качестве автономных и функционально-независимых средств защиты, предназначенных для выявления нарушений политики безопасности ИС. Однако для обеспечения комплексного подхода к информационной безопасности ИС необходимо совместное использование систем обнаружения атак и активного мониторинга рабочих станций ИС. Более подробно варианты такого использования САМ и СОА рассматриваются ниже.

КОМПЛЕКСНОЕ ИСПОЛЬЗОВАНИЕ СИСТЕМ ОБНАРУЖЕНИЯ И АКТИВНОГО МОНИТОРИНГА ИС

Первоначально рассмотрим функциональные различия СОА и САМ на основе следующих показателей: тип используемых датчиков, тип собираемых данных, методы выявления атак и реагирования на них *(см. таблицу)*.

Из данных, представленных в таблице, можно сделать вывод, что САМ являются дополнительным средством для СОА, обеспечивая обнаружение тех атак, которые реализуются внутренними пользователями ИС. Самостоятельно же СОА не могут выявлять такие атаки из-за отсутствия у них механизмов сбора и анализа информации на уровне рабочих станций. С другой стороны, информация, собранная датчиками САМ, может служить и в качестве доказательной базы при проведении расследования инцидентов, связанных с теми нарушениями информационной безопасности ИС, которые были выявлены средствами СОА.

Для демонстрации вышесказанного рассмотрим вариант совместного использования СОА и САМ на конкретном примере. Предположим, что СОА зафиксировала факт проведения сетевой атаки на один из серверов ИС. При этом СОА установила, что атака была проведена с IP-адреса, который принадлежит внутренней рабочей станции пользователя, на которой установлен датчик САМ. Однако знание только IP-адреса не позволяет точно доказать причастность пользователя рабочей станции к проведенной атаке, поскольку адрес станции мог быть преднамеренно искажен нарушителем. В этом случае для подтверждения или опровержения вины пользователя в инциденте могут быть использованы данные, собранные датчиком САМ (регистрационное

Таблица 1. Сравнение систем обнаружения атак и систем активного мониторинга

Тип средства защиты / Показатель сравнения	Системы обнаружения атак	Системы активного мониторинга рабочих станций ИС
Тип используемых датчиков	Сетевые датчики, устанавливаемые в сегменты ИС Хостовые датчики, устанавливаемые на серверы ИС	Хостовые датчики, устанавливаемые на рабочие станции пользователей ИС
Тип собираемых данных	Информация о пакетах данных, передаваемых в ИС	Информация о событиях на рабочих станциях пользователей
Методы выявления атак	Поведенческий метод, основанный на выявлении отклонений от заданных характеристик сетевого трафика ИС Сигнатурный метод, основанный на выявлении в сетевом трафике определенных шаблонов информационных атак	Поведенческий метод, основанный на выявлении нарушений политики безопасности типа «всё, что не разрешено, - запрещено» Сигнатурный метод, основанный на выявлении нарушений политики безопасности типа «всё, что не запрещено, - разрешено»
Методы реагирования	Пассивный метод, обеспечивающий оповещение администратора о выявленных нарушениях Активный метод, обеспечивающий блокирование выявленных сетевых атак	Пассивный метод, обеспечивающий оповещение администратора о выявленных нарушениях Активный метод, обеспечивающий блокирование действий пользователей, нарушающих политику безопасности

имя пользователя, работающего за станцией в момент проведения атаки; перечень приложений, запущенных на станции; информация о сетевом трафике, сформированном запущенными приложениями, и др.). Анализ таких данных позволит определить степень вины пользователя в инциденте. Более того, если выяснится, что пользователь, первоначально попавший под подозрение, невиновен, то анализ информации с других датчиков САМ позволит выявить истинного нарушителя.

Рассмотрим схему размещения СОА и САМ на примере типовой ИС, состоящей из трех сегментов (рис. 3):

- сегмента демилитаризованной зоны, в котором расположены информационные ресурсы, доступные любым внешним и внутренним пользователям ИС;
- сегмента серверов, в котором расположены ресурсы, доступные только внутренним пользователям ИС;
- сегмента рабочих станций пользователей.

Хостовые датчики СОА устанавливаются на все серверы ИС, размещенные в сегментах демилитаризованной зоны и внутренних серверов. Эти датчики обеспечивают обнаружение на прикладном уровне информационных атак тех сетевых служб, которые функционируют на серверах ИС. Сетевые датчики СОА устанавливаются в каждом из сегментов информационной системы для своевременного выявления атак на канальном и сетевом уровнях. Датчики САМ, в свою очередь, устанавливаются на рабочих

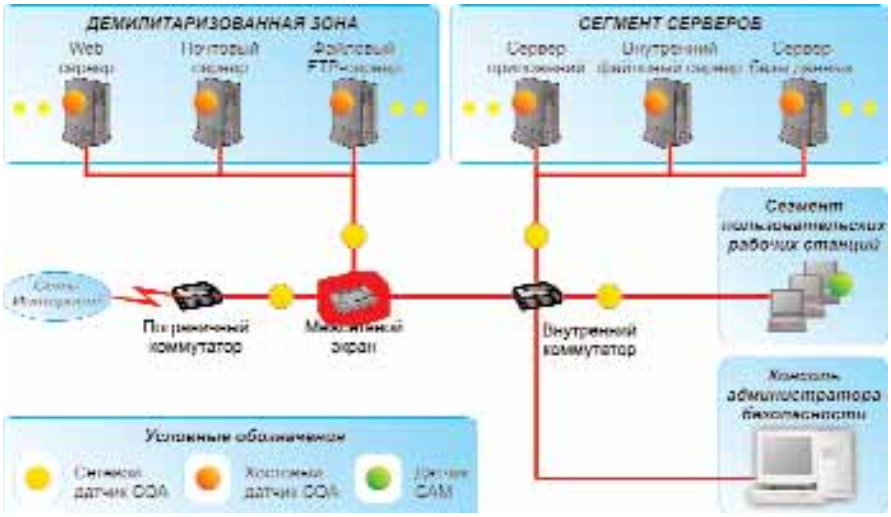

Рис. 3. Схема совместного размещения компонентов СОА и САМ

станциях ИС для выявления несанкционированных действий, нарушающих заданную политику безопасности. Консоль управления СОА и САМ размещается на компьютере администратора безопасности ИС.

ЗАКЛЮЧЕНИЕ И ВЫВОДЫ

Зарождение «пятой колонны» нарушителей информационной безопасности, действующей изнутри ИС, заставляет подвергнуть частичному пересмотру существующую стратегию защиты информационных систем. Учитывая тот факт, что на протяжении длительного времени эта задача решалась лишь при помощи средств разграничения доступа, полностью обеспечить защиту ИС от внутренних нарушителей не представлялось возможным. Это связано с тем, что функциональные возможности этих средств не позволяют защитить ИС от внутренних сетевых атак, а также тех действий внутренних пользователей ИС, которые напрямую не связаны с нарушением правил разграничения доступа к информационным ресурсам системы. Для защиты от внутренних угроз информационной безопасности необходимо использовать СОА и САМ. Датчики СОА размещаются на серверах и рабочих станциях ИС и выполняют функции выявления сетевых атак на основе анализа сетевого трафика. Датчики САМ устанавливаются на рабочие станции пользователей ИС и позволяют выявлять и блокировать те действия пользователей, которые нарушают заданную политику. Совместное использование систем обнаружения атак и активного мониторинга позволит комплексно подойти к вопросу защиты от внутренних атак и значительно повысить уровень информационной безопасности ИС.