Как предотвратить вторжение: второй уровень защиты

Один из важнейших этапов построения комплексной системы защиты информации — создание подсистемы предотвращения вторжений. При этом важен, возможно, не столько выбор средств, сколько грамотное построение второго уровня защиты.

Антон Александров,
менеджер продуктов и решений компании «Элвис-Плюс»

Ни для кого не секрет, что сегодня сотни организаций для обеспечения информационного обмена со своими удаленными филиалами, партнерами, мобильными пользователями и т. д. используют инфраструктуру глобальных внешних сетей (например, Интернета). Однако информационная среда внешних сетей этим организациям неподконтрольна, поэтому такие сети выступают как потенциальный источник сетевых атак, направленных на информационные узлы и ресурсы корпоративных информационных систем (КИС).

Естественно, организации стремятся защитить свои информационные ресурсы. Часто первый уровень защиты КИС от воздействия сетевых атак представляет собой межсетевой экран (МЭ), установленный на стыке с глобальными сетями и фильтрующий потоки данных в соответствии с правилами, определенными политикой безопасности. Большинство современных МЭ позволяют предотвратить воздействие атак, но полной защиты от сетевых атак они не гарантируют. Известно, что некоторые атаки МЭ рассматривает как обычный сетевой поток данных. Например, обращение к Web-серверу для МЭ выглядит как обращение к определенному порту, и весь сетевой поток, предназначенный для данного порта, он обязан пропустить, иначе пользователи не получат доступ к страницам на сервере.

Так что же делать, если атака все-таки прошла защитные механизмы МЭ? Выходом служит применение мер и средств, направленных на обнаружение атаки внутри КИС. Чтобы распознать атаку внутри сетевого потока данных, поступающих на определенный порт, необходимо проанализировать этот поток и по возможности обнаружить атаку до того, как она достигнет конкретной цели. Если удастся выявить атаку внутри КИС, можно будет определить «дыры» в МЭ, а также те виды сетевых атак, которые МЭ пропускает в КИС. Благодаря этому можно правильно настроить МЭ для повышения эффективности его работы.

Но угрозу информационным ресурсам представляют не только действия внешних злоумышленников. Пользователи или администраторы могут своими действиями (целенаправленными или неумышленными) внести нежелательные изменения в конфигурации ПО — это может повлечь за собой зависание ОС, сбои в работе серверов или рабочих станций и т. п. В конечном счете такие изменения ослабляют систему защиты КИС от воздействия атак злоумышленников. Несанкционированно установленные пользователями в пределах КИС модемы позволяют пропускать сетевой трафик в обход средств защиты, что повышает вероятность успеха для атак.

На рынке средств обеспечения информационной безопасности существует отдельный вид решений — системы обнаружения вторжений, или СОВ (Intrusion Detection Systems, IDS), которые в режиме реального времени выявляют атаки внутри КИС. Но просто обнаружить атаку недостаточно — необходимо блокировать ее, предотвратив вредоносное воздействие на ресурсы КИС. Раньше функции блокирования атак возлагались на администратора безопасности — но нельзя гарантировать, что администратор вовремя среагирует и примет соответствующие меры. С недавних пор появился новый вид средств защиты — средства блокирования вторжений, или СБВ (Intru-

sion Protection Systems, IPS), которые уже обеспечивают блокирование атак. Для надежности необходимо оснащать КИС обоими видами средств защиты. Во многих средствах защиты сегодня объединены возможности обнаружения и блокирования вторжений, поэтому их условно называют продуктами СОВ/СБВ.

Но и средств СОВ/СБВ оказывается недостаточно — желательно знать заранее слабые места КИС, называемые в обиходе «дырами», через которые злоумышленник может успешно осуществить атаку. Дырами могут стать «слабые» пароли, несоответствия в настройках сетевых устройств, уязвимости операционных систем и приложений и т. д. Для поиска и выявления такого рода дыр существуют специализированные средства — сканеры уязвимости (vulnerability assessment). Их наличие в КИС существенно повышает уровень защиты: определив слабые места, администратор безопасности может предпринять соответствующие меры по их устранению до того, как злоумышленник воспользуется ими. В последнее время стали появляться специализированные средства, которые обеспечивают автоматический процесс устранения уязвимостей, но пока очень немногие производители предлагают подобные решения.

Чтобы максимально снизить риск негативного воздействия атак, необходимо объединить СОВ, СБВ, сканеры уязвимости и средства устранения уязвимостей в единую подсистему с централизованным управлением — назовем ее подсистемой предотвращения вторжений, ППВ (рис. 1). ППВ в целом и создает второй уровень защиты информационных ресурсов КИС.

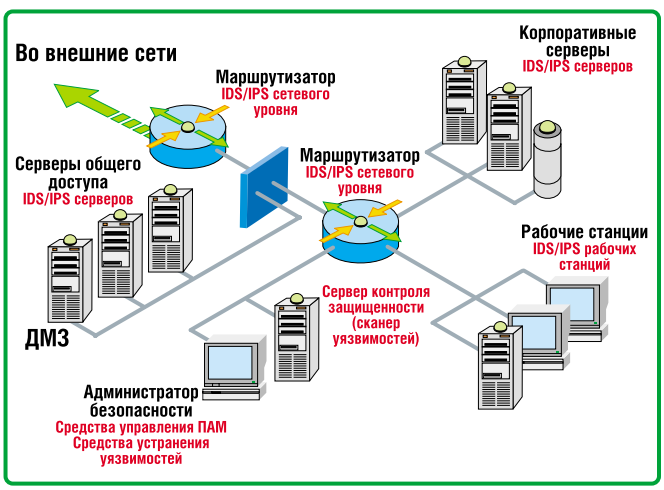

Рис. 1. Подсистема предотвращения вторжений в КИС.

А что говорит мировая статистика и тенденции в данной области безопасности информации? По данным отчета European Information Technology Observatory 2003, 45% компаний в Западной Европе использовали в 2002 г. системы обнаружения атак (в 2001 г. их насчитывалось 35%). Доля компаний, воспользовавшихся сканерами, выросла с 19% в 2001 г. до 35% в 2002 г. Аналитики из Infonetics Research прогнозируют, что доля компаний, использующих эти продукты, к 2007 г. составит 97%.

Функции средств защиты

Для начала обозначим основные функции ППВ в целом. В общем случае эта подсистема осуществляет:

- обнаружение в реальном масштабе времени сетевых атак в потоке данных на различных уровнях КИС — сетевом, уровне информационных узлов;
- блокировку атак до того, как они будут реализованы;
- обнаружение уязвимостей, позволяющих обойти существующие механизмы защиты;
- оперативное оповещение в случае обнаружения атаки и предотвращение ее воздействия;
- устранение (компенсацию) уязвимостей.

Теперь перечислим более подробно функции, возлагаемые на отдельные элементы ППВ.

СОВ и СБВ

С целью обнаружения атак, в том числе идущих изнутри КИС (например, с сервера приложений), эти системы ведут анализ журнала регистрации ОС (syslog) и заданных приложений в реальном времени и/или с некоторой периодичностью, контролируют доступ к файлам и/или их изменения в реальном времени; регистрируют пользовательские действия, изменения учетных данных пользователей, файлов или прав доступа к ним, попытки получить доступ к привилегированным сервисам, изменения политики безопасности и т. д. Они оперативно оповещают администратора о заранее заданных событиях (обнаружение подозрительной сетевой деятельности, обнаружение «слабых» мест) и фактах нарушений политики безопасности, выдают подтверждение факта успешности или неуспешности атаки. Имеется также возможность имитации несуществующих приложений с целью введения злоумышленников в заблуждение.

При обнаружении атак, направленных на серверы и рабочие станции КИС, системы реагируют на них в режиме реального времени (аварийное завершение соединения с атакующим узлом). Возможна корректировка вариантов реагирования на основе анализа событий безопасности перед выполнением каких-либо действий. Имеется функция блокирования учетной записи атакующего пользователя.

Кроме того, системы фиксируют атаки и сохраняют информацию о них, собирают доказательства несанкционированной деятельности злоумышленника (запись протокола атаки в базу, запись всех пакетов через сетевой монитор); обновляют сигнатуры атак; формируют отчеты.

Средства обнаружения уязвимостей

Эти системы выполняют следующие функции: системные проверки настроек, системного доступа, ключевых файлов и т. п.; проверки настроек установленного прикладного ПО, в том числе предназначенного для реализации функций КИС. Проверяется также наличие последних обновлений антивирусного ПО, установленного на серверах и рабочих станциях.

Для определения слабостей парольной системы выполняются проверки типа «подбор пароля» — путем перебора паролей из специальных словарей. Выясняется наличие в системе несанкционированно установленных модемов и других устройств, которые создают реальную угрозу КИС. Ведутся проверки на присутствие «троянских коней», программ для реализации распределенных атак типа «отказ в обслуживании»; средств для реализации атак и подозрительных сетевых приложений (например, анализаторов протоколов) и т. д.

Средства управления

На средства управления возлагаются функции централизованного сбора информации из регистрационных жур-

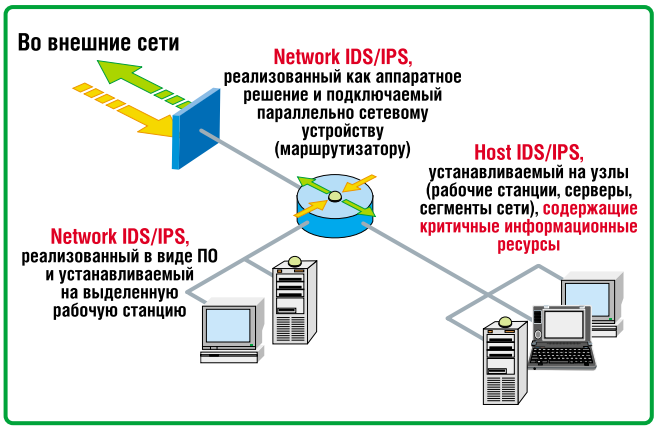

Рис. 2. Типы средств обнаружения и блокирования атак.

налов и систем и управления средствами защиты, входящими в ППВ.

Как работают средства защиты

Теперь рассмотрим, как же работают средства защиты, чтобы обеспечить выполнение перечисленных выше функций.

Различают два типа средств обнаружения и блокирования атак (рис. 2). Системы Host IDS/IPS (Host-based IDS/IPS) действуют на уровне информационных узлов, системы NIDS (Network-based IDS/IPS) — на уровне сети.

Network IDS/IPS (сетевые сенсоры) анализируют сетевой трафик и в случае обнаружения атаки уведомляют систему управления или сами в режиме реального времени блокируют атаку. Для обнаружения используется либо сравнение битовой последовательности проходящего потока данных с эталонным образцом (сигнатурой) атаки, либо фиксация подозрительной (аномальной) сетевой активности посредством анализа сетевого трафика.

Host IDS/IPS (локальные сенсоры) анализируют файлы журнала и ведут мониторинг пользовательской, сетевой и системной активности на узле информационной системы. Логически локальные сенсоры устанавливаются между ядром ОС и пользовательским приложением. Локальные сенсоры перехватывают вызовы, обращенные к системе, сопоставляют их с правилами доступа, определенными политикой безопасности, и затем разрешают или запрещают доступ к ресурсам. Некоторые локальные сенсоры сличают запросы с БД известных сигнатур атак или аномального поведения.

В таблице представлен краткий обзор преимуществ и недостатков Host IDS/IPS и Network IDS/IPS.

Средства контроля текущего состояния и уровня защищенности сетевых объектов, или сетевые сканеры, проводят проверки (регулярные и выборочные) сетевых сервисов, операционных систем, прикладного ПО, маршрутизаторов, межсетевых экранов, Web-серверов и т. п. На основе проведенных проверок сетевые сканеры формируют отчеты с описаниями каждой обнаруженной уязвимости, сведениями о ее расположении на узлах КИС и рекомендациями по коррекции (рис. 3). Отчеты об обнаруженных «слабых местах» КИС служат для устранения найденных уязвимостей. Это можно делать либо с помощью специализированных программных средств (предназначенных в основном для устранения ошибок в настройках ОС и приложениях), либо «вручную», при участии администратора безопасности.

Специализированные программные средства не обеспечивают автоматического устранения всех «слабых» мест в КИС (например, слабости парольной системы) — множество настроек нужно делать вручную, и из-за этого приходится держать в штате компании соответствующего специалиста. Для многих организаций это экономически невыгодно, целесообразнее воспользоваться услугами сторонних специализированных организаций, сотрудники которых будут периодически осуществлять необходимое техническое сопровождение КИС.

Средства устранения уязвимостей в настоящее время имеют узкую область применения — как правило, они поставляются вместе с сетевым окружением и не слишком широко распространены.

Системы управления ППВ обеспечивают взаимодействие средств защиты, входящих в ППВ, а также централизованное управление этими средствами в целях повышения эффективности защиты.

Выбор средств защиты

Для повышения эффективности ППВ необходимо обеспечить тесное взаимодействие всех средств защиты, входящих в эту подсистему. Для этого требуется совместимость всех средств защиты, входящих в ППВ, и единое централизованное управление ими.

Сегодня на мировом рынке средств обнаружения и предотвращения вторжений действуют несколько известных производителей, предлагающих свои решения в данной области. В частности, на российском рынке, по данным CNews (www.cnews.ru), в тройку

лидеров входят компании ISS, Cisco и Symantec.

Применительно к российскому рынку при выборе средств защиты очень важны такие факторы, как наличие у поставщика успешного опыта применения его средств в России (широкая инсталляционная база) и наличие на территории РФ представительств или сертифицированных партнеров, а также развитой системы технической поддержки. Кроме того, желательно, чтобы в ассортименте продуктов поставщика присутствовали средства защиты, покрывающие все уровни ППВ (сетевой, уровни серверов и рабочих станций).

Следует обращать внимание и на другие нюансы. Например, эффективность систем Network IDS/IPS понижается, если скорость обработки потока данных у них ниже, чем пропускная способность сети. Это может привести к пропуску опасного трафика через данные средства защиты. Поэтому к СОВ/СБВ сетевого уровня предъявляются высокие требования по пропускной способности и надежности, а значит, данные средства защиты должны представлять собой аппаратное решение. Более того, зачастую на коммутаторе порты объединяются в VLAN, что не позволяет внешнему (подключаемому к отдельному порту коммутатора) СОВ/СБВ сканировать поток данных, идущий от каждого порта. В результате приходится устанавливать СОВ/СБВ на каждый порт, что экономически невыгодно. Аппаратное решение, встроенное в коммутатор (или маршрутизатор), решает эту проблему.

Следует также учесть, что большинство качественных и полнофункциональных продуктов для обеспечения безопасности второго уровня весьма дороги. Иногда в организации малого и среднего бизнеса достаточно иметь средства анализа защищенности с малым набором функциональных возможностей. Стоимость таких решений на порядок ниже, чем у полнофункциональных. Администратору безопасности достаточно иметь некий автоматизированный инструмент анализа защищенности системы контроля доступа для решения комплекса задач в режиме реального времени: выявления открытых (видимых для всех объектов сети) ресурсов, не предназначенных для общего доступа и использования; проверки паролей на предмет их стойкости к подбору; проверки паролей при аутентификации различных служб TCP/IP (Telnet, FTP, HTTP и др.) и т. д. Немаловажное значение имеет наличие удобного графического интерфейса для просмотра и анализа полученных результатов и формирования отчетов.

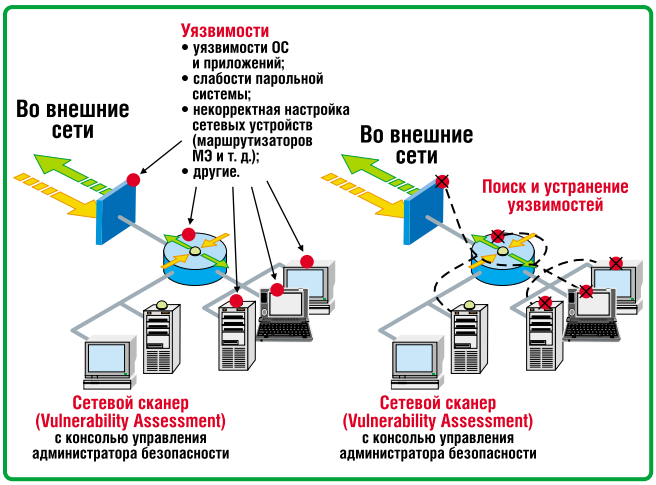

Рис. 3. Схема действия сетевых сканеров.

Преимущества и недостатки разных типов СОВ/СБВ

Преимущества	Недостатки
Network IDS/IPS	
• Широта применения – целая сеть может быть «покрыта» одним сетевым сенсором • Минимальные неудобства от установки обновлений сигнатур и обновлений ПО сенсоров • Предотвращение DoS-атаки • Возможность обнаружения ошибок сетевого уровня в стеке TCP/IP • Независимость от ОС информационных узлов	• Наряду с верными бывают и ложные срабатывания • Не может анализировать зашифрованный поток данных. Новые виды или варианты атак не будут выявлены в случае отсутствия сигнатуры данной атаки • Задержка во времени между моментом обнаружения атаки и моментом оповещения (тревоги) • Затруднен анализ пакетов в случае перегруженной сети • Отсутствуют уведомления об успешности атаки
Host IDS/IPS	
• Возможность связывать пользователя с событием • Может обнаруживать атаки, не обнаруженные сенсорами NIDS • Может проводить анализ данных, расшифрованных на узле • Возможность предоставления информации об узле в течение атаки на него	• Для защиты нескольких узлов сенсоры должны быть установлены на каждом из них • Если ОС «взломана» в результате атаки, то перестает функционировать и сенсор, установленный на данном узле • Сенсор не способен обнаруживать деятельность сетевых сканеров • Сенсоры могут быть неэффективными в случае DoS-атаки на узел • Для функционирования необходимы дополнительные ресурсы

Подобные возможности предоставляет, в частности, система «Застава-Инспектор» производства компании «Элвис-Плюс». В классе продуктов информационной безопасности эта система относится к средствам обнаружения вторжений и атак — она предназначена для оперативного автоматизированного мониторинга открытых информационных ресурсов сети Windows, а также для выявления и предотвращения событий или действий, создающих угрозы безопасности данных. Она не нарушает целостность информационной системы и не требует значительных системных ресурсов. «Застава-Инспектор» может облегчить жизнь администратору безопасности и позволить ему более эффективно выполнять возложенные на него задачи.

В заключение добавим, что наличие второго уровня защиты, реализованного на базе СОВ/СБВ и средств обнаружения уязвимостей, объединенных в подсистему предотвращения вторжений, — это сегодня не роскошь, а насущная необходимость для обеспечения безопасности информационных ресурсов корпоративной информационной системы. Причем проблема для организаций состоит не только в том, какие средства защиты того или иного производителя выбрать, но и как грамотно построить из них второй уровень защиты. B