**Основные понятия**

Под ***протоколированием*** понимается сбор и накопление информации о *событиях*, происходящих в информационной системе. У каждого *сервиса* свой набор возможных событий, но в любом случае их можно разделить на внешние (вызванные действиями других сервисов), внутренние (вызванные действиями самого сервиса) и клиентские (вызванные действиями пользователей и администраторов).

***Аудит*** – это анализ накопленной информации, проводимый оперативно, в реальном времени или периодически (например, раз в день). Оперативный аудит с автоматическим реагированием на выявленные нештатные ситуации называется активным.

Реализация протоколирования и аудита решает следующие задачи:

* обеспечение *подотчетности* пользователей и администраторов;
* обеспечение возможности реконструкции последовательности событий;
* обнаружение попыток *нарушений информационной безопасности*;
* предоставление информации для выявления и анализа проблем.

Протоколирование требует для своей реализации здравого смысла. Какие события регистрировать? С какой степенью *детализации*? На подобные вопросы невозможно дать универсальные ответы. Необходимо следить за тем, чтобы, с одной стороны, достигались перечисленные выше цели, а, с другой, расход ресурсов оставался в пределах допустимого. Слишком обширное или подробное протоколирование не только снижает производительность сервисов (что отрицательно сказывается на *доступности*), но и затрудняет аудит, то есть не увеличивает, а уменьшает информационную безопасность.

Разумный подход к упомянутым вопросам применительно к операционным системам предлагается в "*Оранжевой книге*", где выделены следующие события:

* вход в систему (успешный или нет);
* выход из системы;
* обращение к удаленной системе;
* операции с файлами (открыть, закрыть, переименовать, удалить);
* смена привилегий или иных атрибутов безопасности (режима доступа, уровня благонадежности пользователя и т.п.).

При протоколировании события рекомендуется записывать, по крайней мере, следующую информацию:

* дата и время события;
* уникальный идентификатор пользователя – инициатора действия;
* *тип события*;
* результат действия (успех или неудача);
* источник запроса (например, *имя терминала*);
* имена затронутых объектов (например, открываемых или удаляемых файлов);
* описание изменений, внесенных в базы данных защиты (например, новая *метка безопасности* объекта).

Еще одно важное понятие, фигурирующее в "*Оранжевой книге*", – *выборочное протоколирование*, как в отношении пользователей (внимательно следить только за подозрительными), так и в отношении событий.

Характерная особенность протоколирования и аудита – зависимость от других средств безопасности. *Идентификация и аутентификация* служат отправной точкой *подотчетности* пользователей, логическое управление доступом защищает конфиденциальность и целостность *регистрационной информации*. Возможно, для защиты привлекаются и криптографические методы.

Возвращаясь к целям протоколирования и аудита, отметим, что обеспечение *подотчетности* важно в первую очередь как сдерживающее средство. Если пользователи и администраторы знают, что все их действия фиксируются, они, возможно, воздержатся от незаконных операций. Очевидно, если есть основания подозревать какого-либо пользователя в нечестности, можно регистрировать все его действия, вплоть до каждого нажатия клавиши. При этом обеспечивается не только возможность расследования случаев нарушения режима безопасности, но и откат некорректных изменений (если в протоколе присутствуют данные до и после модификации). Тем самым защищается целостность информации.

Реконструкция последовательности событий позволяет выявить слабости в защите сервисов, найти виновника вторжения, оценить масштабы причиненного ущерба и вернуться к нормальной работе.

Обнаружение попыток *нарушений информационной безопасности* – функция активного аудита, о котором пойдет речь в следующем разделе. Обычный аудит позволяет выявить подобные попытки с опозданием, но и это оказывается полезным. В свое время поимка немецких хакеров, действовавших по заказу КГБ, началась с выявления подозрительного расхождения в несколько *центов* в ежедневном отчете крупного вычислительного центра.

Выявление и анализ проблем могут помочь улучшить такой параметр безопасности, как доступность. Обнаружив узкие места, можно попытаться переконфигурировать или перенастроить систему, снова измерить производительность и т.д.

Непросто осуществить организацию согласованного протоколирования и аудита в распределенной разнородной системе. Во-первых, некоторые компоненты, важные для безопасности (например, маршрутизаторы), могут не обладать своими ресурсами протоколирования; в таком случае их нужно экранировать другими сервисами, которые возьмут протоколирование на себя. Во-вторых, необходимо увязывать между собой события в разных сервисах.

### Активный аудит

#### Основные понятия

Под ***подозрительной активностью*** понимается поведение пользователя или компонента информационной системы, являющееся ***злоумышленным*** (в соответствии с заранее определенной политикой безопасности) или нетипичным (согласно принятым критериям).

Задача активного аудита – оперативно выявлять *подозрительную активность* и предоставлять средства для *автоматического реагирования*на нее.

Активность, не *соответствующую политике безопасности*, целесообразно разделить на *атаки*, направленные на незаконное получение полномочий, и на действия, выполняемые в рамках имеющихся полномочий, но нарушающие политику безопасности.

Атаки нарушают любую осмысленную политику безопасности. Иными словами, *активность атакующего* является разрушительной независимо от политики. Следовательно, для описания и выявления атак можно применять *универсальные методы*, инвариантные относительно политики безопасности, такие как сигнатуры и их обнаружение во входном потоке событий с помощью аппарата *экспертных систем*.

***Сигнатура атаки*** – это совокупность условий, при выполнении которых атака считается имеющей место, что вызывает заранее определенную реакцию. Простейший пример сигнатуры – "зафиксированы три последовательные неудачные попытки входа в систему с одного терминала", пример ассоциированной реакции – блокирование терминала до прояснения ситуации.

Действия, выполняемые в рамках имеющихся полномочий, но нарушающие политику безопасности, мы будем называть *злоупотреблением полномочиями*. *Злоупотребления полномочиями* возможны из-за неадекватности средств разграничения доступа выбранной политике безопасности. Простейшим примером злоупотреблений является неэтичное поведение суперпользователя, просматривающего личные файлы других пользователей. Анализируя регистрационную информацию, можно обнаружить подобные события и сообщить о них *администратору безопасности*, хотя для этого необходимы соответствующие средства выражения политики безопасности.

Выделение злоупотреблений полномочиями в отдельную группу неправомерных действий, выявляемых средствами активного аудита, не является общепринятым, однако, на наш взгляд, подобный подход имеет право на существование и мы будем его придерживаться, хотя наиболее радикальным решением было бы развитие средств разграничения доступа (см. "Возможный подход к управлению доступом в распределенной объектной среде").

Нетипичное *поведение* выявляется статистическими методами. В простейшем случае применяют систему *порогов*, превышение которых является подозрительным. (Впрочем, "пороговый" метод можно трактовать и как вырожденный случай сигнатуры атаки, и как тривиальный способ выражения политики безопасности.) В более развитых системах производится сопоставление долговременных характеристик работы (называемых *долгосрочным профилем* ) с *краткосрочными профилями*. (Здесь можно усмотреть аналогию биометрической аутентификации по поведенческим характеристикам.)

Применительно к средствам активного аудита различают *ошибки первого* и *второго рода*: *пропуск атак* и *ложные тревоги*, соответственно. Нежелательность ошибок первого рода очевидна; ошибки второго рода не менее неприятны, поскольку отвлекают администратора безопасности от действительно важных дел, косвенно способствуя *пропуску атак*.

Достоинства *сигнатурного метода* – высокая производительность, малое число ошибок второго рода, обоснованность решений. Основной недостаток – неумение обнаруживать неизвестные атаки и вариации известных атак.

Основные достоинства статистического подхода – универсальность и обоснованность решений, потенциальная способность обнаруживать неизвестные атаки, то есть минимизация числа ошибок первого рода. Минусы заключаются в относительно высокой доле ошибок второго рода, плохой работе в случае, когда неправомерное поведение является типичным, когда типичное поведение плавно меняется от легального к неправомерному, а также в случаях, когда типичного поведения нет (как показывает статистика, таких пользователей примерно 5-10%).

Средства активного аудита могут располагаться на всех линиях обороны информационной системы. На границе контролируемой зоны они могут обнаруживать *подозрительную активность* в точках подключения к внешним сетям (не только попытки нелегального проникновения, но и действия по "прощупыванию" *сервисов безопасности*). В корпоративной сети, в рамках *информационных сервисов* и *сервисов безопасности*, *активный аудит* в состоянии обнаружить и пресечь *подозрительную активность* внешних и внутренних пользователей, выявить проблемы в работе сервисов, вызванные как нарушениями безопасности, так и аппаратно-программными ошибками. Важно отметить, что *активный аудит*, в принципе, способен обеспечить защиту от атак на доступность.

К сожалению, формулировка "в принципе, способен обеспечить защиту" не случайна. *Активный аудит* развивается более десяти лет, и первые результаты казались весьма многообещающими. Довольно быстро удалось реализовать распознавание простых типовых атак, однако затем было выявлено множество проблем, связанных с обнаружением заранее неизвестных атак, атак распределенных, растянутых во времени и т.п. Было бы наивно ожидать полного решения подобных проблем в ближайшее время. (Оперативное пополнение базы сигнатур атак таким решением, конечно, не является.) Тем не менее, и на нынешней стадии развития *активный аудит* полезен как один из рубежей (вернее, как набор прослоек) *эшелонированной обороны*.

#### Функциональные компоненты и архитектура

В составе средств активного аудита можно выделить следующие функциональные компоненты:

* компоненты генерации *регистрационной информации*. Они находятся на стыке между средствами активного аудита и контролируемыми объектами;
* компоненты хранения сгенерированной *регистрационной информации*;
* компоненты извлечения *регистрационной информации* ( *сенсоры* ). Обычно различают сетевые и хостовые сенсоры, имея в виду под первыми выделенные компьютеры, сетевые карты которых установлены в режим прослушивания, а под вторыми – программы, читающие регистрационные журналы операционной системы. На наш взгляд, с развитием коммутационных технологий это различие постепенно стирается, так как сетевые сенсоры приходится устанавливать в активном сетевом оборудовании и, по сути, они становятся частью*сетевой ОС*;
* компоненты просмотра *регистрационной информации*. Могут помочь при принятии решения о реагировании на *подозрительную активность*;
* компоненты *анализа* информации, поступившей от сенсоров. В соответствии с данным выше определением средств активного аудита, выделяют пороговый анализатор, анализатор нарушений политики безопасности, экспертную систему, выявляющую *сигнатуры атак*, а также статистический анализатор, обнаруживающий нетипичное поведение;
* компоненты хранения информации, участвующей в анализе. Такое хранение необходимо, например, для выявления атак, протяженных во времени;
* компоненты принятия решений и реагирования (" *решатели* "). "*Решатель*" может получать информацию не только от локальных, но и от внешних анализаторов, проводя так называемый корреляционный анализ распределенных событий;
* компоненты хранения информации о контролируемых объектах. Здесь могут храниться как пассивные данные, так и методы, необходимые, например, для извлечения из объекта *регистрационной информации* или для реагирования;
* компоненты, играющие роль организующей оболочки для менеджеров активного аудита, называемые мониторами и объединяющие анализаторы, "*решатели*", хранилище описаний объектов и *интерфейсные* компоненты. В число последних входят компоненты интерфейса с другими мониторами, как равноправными, так и входящими в иерархию. Такие интерфейсы необходимы, например, для выявления распределенных, широкомасштабных атак;
* компоненты интерфейса с *администратором безопасности*.

Средства активного аудита строятся в архитектуре *менеджер* / *агент*. Основными агентскими компонентами являются сенсоры. Анализ, принятие решений – функции менеджеров. Очевидно, между менеджерами и агентами должны быть сформированы доверенные каналы.

Подчеркнем важность интерфейсных компонентов. Они полезны как с внутренней для средств активного аудита точки зрения (обеспечивают расширяемость, подключение компонентов различных производителей), так и с внешней точки зрения. Между менеджерами (между компонентами анализа и "решателями") могут существовать горизонтальные связи, необходимые для анализа распределенной активности. Возможно также формирование иерархий средств активного аудита с вынесением на верхние уровни информации о наиболее масштабной и опасной активности.

Обратим также внимание на архитектурную общность средств активного аудита и управления, являющуюся следствием общности выполняемых функций. Продуманные интерфейсные компоненты могут существенно облегчить совместную работу этих средств.