КОМПЛЕКСНОЕ УПРАВЛЕНИЕ ИНФОРМАЦИОННЫМИ РИСКАМИ

Антон Александров,
менеджер продуктов и решений ОАО «ЭЛВИС-ПЛЮС»

BYTE, 10 июня 2004 г.

В современных информационных системах (ИС) практически любой компании присутствуют средства защиты, позволяющие реализовать различные службы безопасности информации и решающие определенные задачи защиты информационных ресурсов. К самым распространенным на сегодня средствам защиты относятся межсетевые экраны, средства антивирусной защиты и средства предотвращения вторжений - как на уровне отдельно взятого информационного узла (хоста), так и на уровне ИС в целом. Одна из главных составляющих функционирования таких средств - процедура регистрации и последующей обработки событий безопасности (регистрационных данных), причем для средств предотвращения вторжений данная процедура имеет характер ключевой.

Сами регистрационные данные дают возможность анализировать взаимодействие ИС с внешними сетями (внешними пользователями): выявлять слабые места ИС (уязвимости), обнаруживать несанкционированные или недопустимые действия и другие вредоносные воздействия как со стороны внешней информационной среды, так и изнутри (внутренние пользователи). Все это обеспечивает мониторинг состояния ИС с точки зрения информационной безопасности в режиме реального времени. Регистрационные данные, создаваемые операционными системами или приложениями, также служат носителями ценной информации и безусловно заслуживают не меньшего внимания.

Хорошо известно, что в состав ИС, особенно крупных, может входить несколько разных средств защиты и операционных систем, регистрирующих события безопасности. Это порождает огромные объемы анализируемой информации (до 10 Гбайт в час). В результате компании оказываются перед выбором: либо содержать несколько высококлассных специалистов-аналитиков в области информационной безопасности, чтобы анализировать события, поступающие от каждого устройства, либо игнорировать большинство событий безопасности. Первый вариант, очевидно, слишком "дорогое удовольствие", и он не всегда возможен ввиду отсутствия специалистов. Второй подход просто недопустим, он явно сводит на нет все усилия по защите информационных ресурсов компании - вплоть до того, что факт подготовки к осуществлению атаки или самой атаки будет просто пропущен.

Стоит заметить, что обычно объектом атаки злоумышленника становится не отдельная подсистема (подсистемы), а ИС в целом. При этом атаки могут иметь как целевой (изолированный) характер, так и общесетевой; могут быть и быстротечными, и достаточно распределенными во времени. Поэтому эффективный анализ должен носить комплексный характер, т. е. изучаться должен максимально возможный набор событий безопасности (поступающих от устройств, распределенных по всей ИС), а кроме того, нужна возможность их исторического анализа. Задача такого комплексного и централизованного анализа становится непосильной для любого ИТ-специалиста.

Таким образом, в ИС, где вырабатывается множество событий безопасности, необходимо предусмотреть специализированные средства, которые решали бы задачу автоматизации централизованного анализа содержимого регистрационных файлов, т. е. задачу комплексного управления информационными рисками. Причем, что не менее важно, средства управления рисками должны качественно отличать реальные атаки от каких-либо безвредных действий, чтобы исключить ложные срабатывания, и качественно обнаруживать атаку, не давая ей распространяться дальше. Например, нужно уметь различать случай многократного ввода неправильного пароля пользователем (если он его забыл) и случай подбора пароля злоумышленником.

Анализ - это, конечно же, хорошо, но достаточно ли только анализа? Учитывая скорости реализации атаки, необходимо, чтобы средства защиты не только выполняли функции анализа событий, но и обеспечивали быстрое реагирование при обнаружении подозрительных событий: например, запуска процесса блокирования портов на межсетевом экране, запрета сетевого соединения и т. д. Кроме того, в целях повышения эффективности следует предусмотреть процедуру поддержки принятия решения. Данная функция призвана выдавать запрограммированные результаты обработки опасных событий, в которых содержатся своего рода рекомендации по устранению атаки или уменьшению ее отрицательного воздействия на информационные ресурсы системы.

Система управления информационными рисками

Итак, перейдем к главному вопросу: каким образом применить специализированные средства анализа событий, чтобы реализовать в ИС управление информационными рисками? Прежде всего, поскольку анализ носит комплексный характер, такие средства должны объединяться в отдельную подсистему - подсистему управления информационными рисками (ПУИР), компоненты которой распределены по всей ИС. В общем случае эта подсистема предназначена для автоматизации комплексного анализа содержимого регистрационных файлов и управления информационными рисками ИС. Она последовательно выполняет следующие действия.

Сбор регистрационных данных. В случае появления новой регистрационной записи (поступившей от средства защиты, ОС, приложения и т. д.) в режиме реального времени проводится ее прием и выборка в соответствии с задаваемыми правилами (например, выбираются только определенные поля из регистрационной записи).

Преобразование и отправка событий. Собранные регистрационные данные преобразуются в необходимый для последующей обработки единый формат события, и эти события последовательно отправляются средству обработки.

Соотношение (корреляционный анализ) событий. Полученные события централизованно проходят процедуру корреляционного анализа. Под корреляционным анализом понимается совокупная обработка событий с целью выявления событий, заслуживающих внимания (попытка несанкционированного доступа, DoS-атака), и событий, не несущих в себе опасности, которые можно удалить. Выделенные события помещаются в базу данных.

Графическое отображение событий. События выбираются из базы данных и отображаются на консоли специалиста-аналитика.

Учитывая особенности функционирования ПУИР, целесообразно строить подсистему, в состав которой входили бы следующие компоненты (рис. 1):

- средства (агенты);
- сервер обработки событий (СОС);
- база данных (хранилище событий);
- графическая консоль.

Рис. **1.** Логическая схема ПУИР.

Вообще говоря, в состав ПУИР следовало бы включить и источники событий безопасности: операционные системы, средства защиты, средства коммутации - все устройства, формирующие регистрационные данные. Однако в рамках самой подсистемы источники следует рассматривать как объекты, с которыми тесно взаимодействуют ее агенты, иначе границы и функциональность ПУИР нельзя будет четко определить. Сами агенты распределены по всей ИС (в общем случае они устанавливаются на источники событий) и обеспечивают локальный сбор информации (из регистрационных данных), их первоначальную фильтрацию и преобразование в формат, необходимый для последующего анализа (корреляции) на сервере обработки

событий (СОС). В свою очередь, СОС принимает преобразованные данные (события) от всех агентов, входящих в ПУИР, обеспечивает их корреляционный анализ и помещает результаты анализа в базу данных. Хранилище событий обеспечивает хранение обработанных на СОС данных и позволяет осуществлять исторический анализ на основе хранимых событий. И, наконец, графическая консоль представляет собой средство графического отображения результатов анализа событий.

Как выбирать ПО

Выбор средств управления рисками - важнейший момент при построении ПУИР. При выборе ПО, выполняющего основные функции подсистемы, необходимо учитывать разнообразные критерии, оценивая, например, не только первичную стоимость продуктов, но и затраты на их сопровождение, продление лицензий и техническую поддержку.

Общие требования

К основным параметрам, по которым оценивается качество ПО, используемого для построения ПУИР, можно отнести:

- полноту набора функций;
- совместимость с различными средствами защиты третьих фирм;
- совместимость с различными аппаратными платформами;
- совместимость с различными ОС;
- возможность поддержки принятия решений для последующих корректных настроек средств защиты;
- наличие у производителя официальных представительств или сертифицированных партнеров на территории РФ;
- наличие развитой сети технической поддержки на территории РФ.

Технические требования

Исходя из задач, которые возлагаются на внедряемую подсистему в ИС, она должна обеспечивать выполнение следующих действий:

- просмотр и сбор информации из регистрационных файлов, создаваемых источниками событий;
- фильтрацию и выборку событий в соответствии с правилами обработки событий;
- анализ и согласование (корреляцию) собранных данных;
- отправку наиболее важных событий в точку сбора (на консоль администратора безопасности);
- исторический анализ обработанных событий;
- архивацию (ведение базы данных) обработанных событий, результатов их обработки, процедур реагирования на инциденты и т. д.

Система должна также выполнять запрограммированные действия (отключение сетевого соединения, запрет определенных правил фильтрации и т. д.) при наличии определенных событий (DoS-атака, попытка несанкционированного доступа и т. п.).

Дополнительные требования

Перечисленные ниже возможности не относятся к обязательным требованиям, но их наличие желательно и заметно повышает привлекательность продукта при выборе. В числе таких характеристик назовем следующие:

- возможность построения иерархической структуры ПУИР (центральный офис - филиалы);
- поддержка распространенных платформ и стандартов;
- наличие предустановленных правил фильтрации и обработки событий;
- удобные и гибкие средства просмотра результатов обработки и создания отчетов;
- возможность создания дополнительных фильтров, ответных действий и собственных правил обработки событий безопасности (процедур);
- поддержка распространенных форматов передачи событий безопасности.

Tivoli Risk Manager

Рынок средств анализа событий безопасности и управления информационными рисками еще довольно новый. В России пока представлено сравнительно немного производителей такого рода средств. Один из наиболее известных продуктов - Tivoli Risk Manager компании IBM (http://www.ibm.com), который полностью отвечает перечисленным выше требованиям.

Risk Manager позволяет с единой консоли управлять информационными рисками в ИС. В нем реализована возможность централизованного обнаружения и оценки возможных и реальных угроз информационным ресурсам путем согласования (корреляции) событий безопасности, поступающих с межсетевых экранов, маршрутизаторов, сетевых и локальных сенсоров (IDS/IPS), информационных узлов и сканеров безопасности. Централизованным же образом ведется архив событий безопасности в реляционной базе данных. Возможно расширение (масштабирование) инфраструктуры управления событиями, поступающими от различных источников. Существует также возможность оценки состояния безопасности беспроводных сегментов (wireless LAN).

Единая корпоративная графическая консоль Risk Manager обеспечивает в режиме реального времени просмотр (визуализацию) и управление событиями безопасности. Графическое отображение событий помогает аналитикам и другим ИТ-специалистам оценивать состояние безопасности ИС и оперативно принимать решения, уменьшающие или устраняющие влияние различных рисков.

В Risk Manager встроена поддержка принятия решений, включающая предопределенные отчеты для оперативного изменения и последующей оптимальной настройки средств защиты.

Пакет Risk Manager состоит из следующих основных компонентов:

- источники событий (Event Sources);
- адаптер событий (Event Adapters);
- клиенты RM (Tivoli Risk Manager Clients);
- сервер событий (Tivoli Risk Manager Event Server);
- графическая консоль (Tivoli Risk Manager Console);
- средство выдачи отчетов (Tivoli Risk Manager Historical Reporting);
- база данных событий (Tivoli Event Repository).

Как было сказано выше, источники событий не входят в подсистему. В составе продукта они указаны потому, что в пакете Risk Manager предусмотрено наличие таких компонентов, если в ИС отсутствуют необходимые источники. Роль агента ПУИР в Risk Manager выполняют устанавливаемые вместе и функционирующие на одном хосте адаптер и клиент. Средство выдачи отчетов обеспечивает наглядное представление результатов анализа в формате Crystal Reports.

Рассмотрим подробнее процесс обработки событий, поступающих от источников событий, в Risk Manager.

Обнаружение. Допустим, сенсор IDS или приложение обнаруживает подозрительную активность или другие действия, заслуживающие внимания с точки зрения информационной безопасности. После этого событие регистрируется.

Фильтрация и суммирование. Адаптер Risk Manager перехватывает сообщение источника, преобразует его в необходимый формат и перенаправляет его на клиент RM, который удаляет одинаковые и дублирующие друг друга события (логическое суммирование событий). После этого событие направляется на сервер событий.

Первый уровень корреляции. На этом уровне используется механизм корреляции на базе состояния, который проводит поиск шаблона активности. Если поиск дал положительный результат, вырабатывается событие-инцидент, представляющее собой "снимок" шаблона подозрительной активности, появившейся в определенный промежуток времени. Событие-инцидент направляется для дальнейшей обработки на второй уровень.

Второй уровень корреляции. На этом уровне используются пролог-правила для дальнейшей фильтрации уже тех событий-инцидентов, которые приходят от одного или нескольких (в случае распределенной структуры Risk Manager) механизмов корреляции первого уровня.

Структура ПУИР

Посмотрим, как выглядит подсистема ПУИР, построенная на основе Risk Manager. Ядром ее (рис. 2) служит сервер TEC, для установки которого необходимо наличие инфраструктуры Tivoli (Tivoli Framework). Для реализации функций СОС на сервер TEC устанавливается программный компонент Risk Manager, обеспечивающий обработку поступающих событий в соответствии с правилами, реализованными корреляционным механизмом Risk Manager. Для хранения событий, поступающих от адаптеров Risk Manager, предусмотрена реляционная база данных, которая для повышения производительности обработки устанавливается на отдельный сервер.

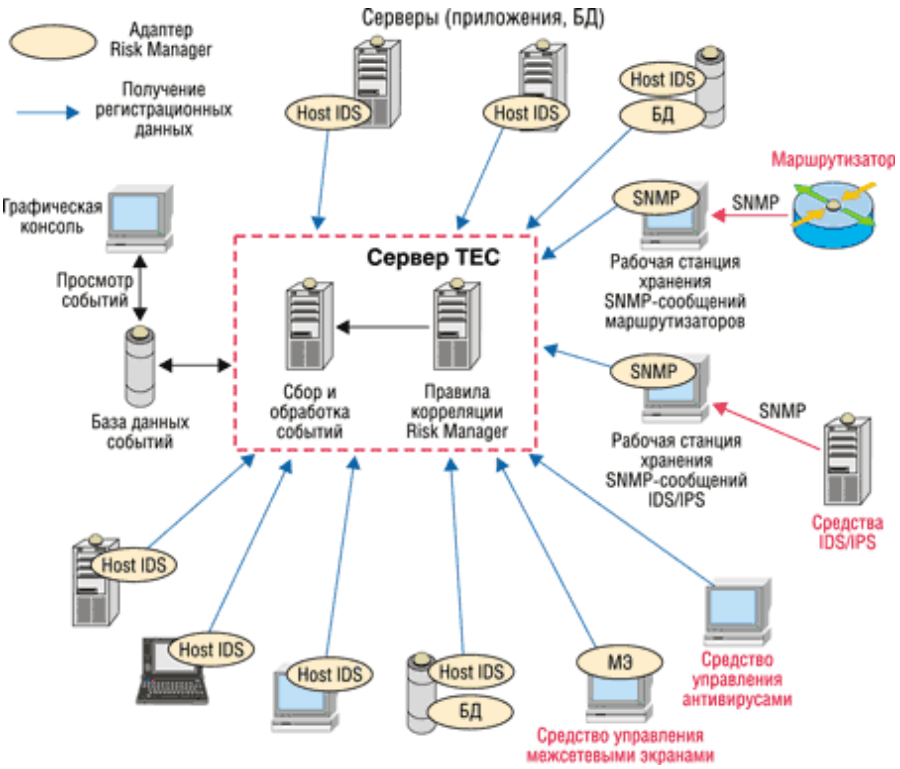

Рис. 2. Архитектура ПУИР.

В общем случае на серверы ИС устанавливаются клиенты Risk Manager, в состав которых входят адаптеры и клиенты для следующих компонентов ИС:

- операционных систем - выбирают события из файлов системных журналов;
- антивирусных пакетов - выбирают события из журналов, генерируемых компонентом антивирусного пакета или средством централизованного управления антивирусами;
- баз данных - выбирают события непосредственно из таблиц БД;
- SNMP-сообщений - выбирают сообщения, посылаемые средствами защиты на отдельную рабочую станцию по SNMP-протоколу (маршрутизаторы, IDS/IPS и т. д.);
- межсетевых экранов - выбирают события из журналов, генерируемых самим межсетевым экраном или средством централизованного управления им.

Адаптеры работают в режиме, который предусматривает поставку и последующую установку адаптера вместе с клиентом (режим non-TME). Клиент получает от своего адаптера отформатированные данные, проводит их логическое суммирование и направляет на сервер TEC для последующей обработки. Адаптеры Host IDS для различных ОС обнаруживают потенциально опасные события, записанные в файлах системных

журналов, преобразуют их и посредством клиента посылают на сервер событий. Целесообразно в первую очередь устанавливать адаптеры на те серверы и рабочие станции, которые обрабатывают критичную информацию.

В зависимости от механизма создания и хранения регистрационных данных различными средствами защиты, установленными в ИС, регистрационные данные получают разными способами - либо централизованно, от средства коллективного сбора регистрационных данных (зачастую это средство централизованного управления), либо локально, непосредственно от самого средства защиты (если это возможно).

Выводы

В настоящее время некоторые средства защиты вышли на тот уровень "разумности", когда решение многих задач, которые раньше выполнял человек, можно полностью автоматизировать и предоставить их выполнение компьютеру. Конечно же, "компьютерному разуму" еще далеко до человека, и многие задачи ему не по плечу. Однако в случае задачи комплексного анализа именно вычислительная мощь компьютера (естественно, при наличии специализированного ПО) становится решающим фактором.

Решение на базе продукта IBM Tivoli Risk Manager позволяет создать комплексную подсистему управления информационными рисками, существенно повысив уровень защищенности информационных ресурсов и обеспечив защиту инвестиций в инфраструктуру безопасности. Однако из-за сложности решения и наличия множества системных компонентов окончательный вариант решения для создания ПУИР в конкретной ИС требует технического проектирования.
