УДК 004.4

АРХИТЕКТУРА, ВЗАИМОДЕЙСТВИЕ КОМПОНЕНТОВ, ПРЕИМУЩЕСТВА SITEPROTECTOR

Александр Голяка
НБУ

Аннотация: **Представлена архитектура системы SiteProtector.**
Summary: **Architecture of the system SiteProtector is presented.**
Ключевые слова: **Системы обнаружения вторжений, SiteProtector.**

Больше половины компаний во всем мире используют системы обнаружения вторжений (СОВ) для защиты своих внешних и внутренних ресурсов. На лидирующие позиции в этом сегменте рынка претендуют две компании – Cisco Systems и Internet Security Systems. Эта тенденция прослеживается как в западном, так и в отечественном секторах. В статье [1] приводятся результаты исследований применения различных методов СОВ для обнаружения атак на ИТС. Рассмотрим как реализованы эти методы в конкретном типовом решении – системе SiteProtector, являющейся решением СОВ от компании Internet Security Systems. Для исчерпывающего описания технологии обнаружения атак считаем необходимым рассмотреть следующие аспекты: методы получения СОВ информации об атаках, анализ полученных данных, архитектуру системы, способы реагирования на атаку.

Архитектура SiteProtector

Типичная установка SiteProtector, рассчитанная на один или несколько компьютеров, изображена на рис. 1.

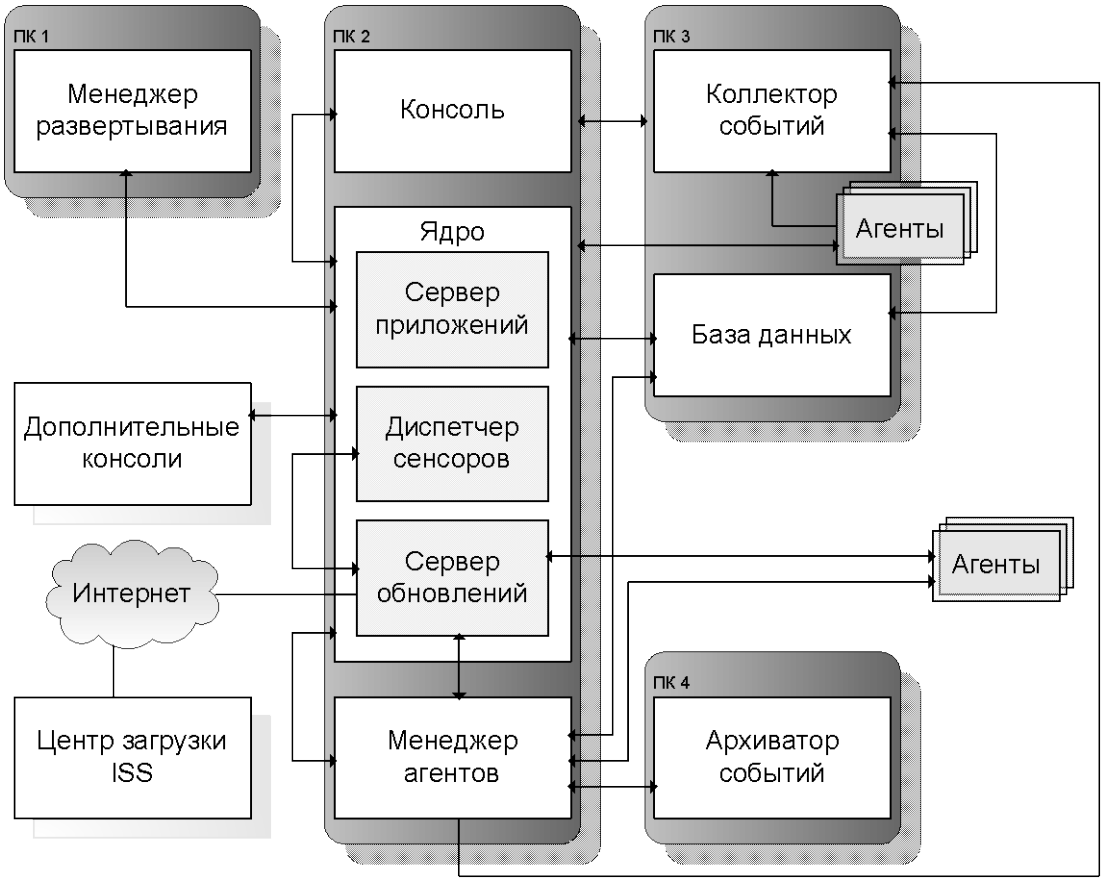

Рисунок 1 – SiteProtector

SiteProtector состоит из базовых и опциональных компонентов, обеспечивающих необходимую функциональность для доступа, мониторинга и анализа событий сети.

- Коллектор событий (Event Collector).

Отвечает за сбор сигналов тревоги от всех управляемых сканеров безопасности Internet Scanner и System Scanner, агентов RealSecure Desktop, сенсоров RealSecure Network 10/100, Gigabit Network, Server и Proventia A и G, а также межсетевых экранов Check Point Firewall-1 и Cisco Pix. Полученные сигналы тревоги передаются на хранение в базу данных.

В крупных, территориально распределенных сетях возможно использование до 5 менеджеров событий, объединенных единой базой данных. Такая возможность позволяет более эффективно управлять событиями, передаваемыми из удаленных филиалов корпоративной сети по каналам связи, построить отказоустойчивую конфигурацию, позволяющую в случае выхода из строя основного менеджера переключаться на резервный.

- База данных (Enterprise Database).

Отвечает за хранение сигналов тревоги, получаемых от одного или нескольких коллекторов событий; статистики событий безопасности; командные и управляемые данные; статус X-Press Updates. Функционирование под управлением MS SQL Server позволяет обеспечить надежное хранение собранных данных, а также отказоустойчивость базы данных за счет встроенных возможностей.

- Сервер приложений (Application Server).

Отвечает за взаимодействие между базой данных событий и консолью правления, а также за посылку команд управления всем сенсорам. Этот же компонент отвечает за централизованное хранение всех обновлений X-Press Updates и политик безопасности, распределяемых среди сенсоров.

Механизм X-Press Update позволяет автоматически и своевременно получать обновления базы данных сигнатур атак и уязвимостей по защищенному от несанкционированного доступа каналу. Процесс обновления полностью автоматизирован и выполняется в заданное администратором время. По умолчанию интервал обновления составляет 24 часа, однако эта цифра может быть изменена администратором системы. Помимо загрузки обновлений, система управления распределяет их (также в автоматическом режиме) среди всех подключенных в данный момент сканеров безопасности Internet Scanner, агентов RealSecure Desktop и сенсоров Proventia, RealSecure Network 10/100, Gigabit Network и RealSecure Server. Если по каким-то причинам удаленный компонент в момент обновления неактивен, то это задание откладывается до момента его активизации. Все обновления защищены от несанкционированного изменения и распределяются только после прохождения процесса аутентификации между сервером обновления и системой управления, а также между системой управления и агентами. В качестве сервера обновлений может выступать как Web-сервер компании Internet Security Systems или внутренний корпоративный портал компании, так и сетевой или локальный диск, на которых хранятся все обновления X-Press Update. При помощи этого же механизма возможно обновление компонентов решений компании ISS для расширения их функциональных возможностей (новые отчеты, новые функции ядра и т. д.). Этот механизм позволяет администратору не тратить время на необходимость обновления средств защиты, т. к. система управления берет эту задачу полностью на себя.

- Графическая консоль управления (Console).

Отвечает за визуализацию событий от управляемых средств защиты. В состав консоли управления входят следующие компоненты: Site Manager – обеспечивает управление одним RSSP; Enterprise Dashboard – обеспечивает анализ и сравнения данных, собранных SiteManager'ом.

SiteManager'ы могут быть установлены и в удаленных филиалах. При этом, используя механизм фильтрации, они могут отображать не все события, позволяя администратору безопасности сконцентрироваться только на тех событиях, которые относятся к данному филиалу.

Компонент Enterprise Dashboard позволяет обеспечивать более высокий уровень анализа данных от различных управляемых средств защиты, сравнивать уровни защищенности, изучать тенденции и т. п.

- Менеджер агентов (Agent Manager, в прошлых версиях комплекса назывался Desktop Controller).

Предназначен для сбора сигналов тревоги и информации от агентов RealSecure Desktop и RealSecure Desktop Enforcement for VPN, защищающих рабочие станции и переносные компьютеры, также Proventia G и M, Архиватора событий, X-Press Update Server и передачу данных от агентов до коллектора событий. Через этот же компонент на управляемые агенты передаются все команды управления и т. д.

- Менеджер развертывания (Deployment Manager).

Является Веб-сервером, позволяющим инсталлировать любые компоненты SiteProtector'а и агенты на компьютеры сети.

- Архиватор событий (Event Archiver).

Обеспечивает возможность архивировать события безопасности в удаленном расположении.

- Ядро (Core).

Обеспечивает связь между консолью и базой данных, управление командами и работой агентов.

Агенты, отвечающие за сбор информации и обнаружение атак, делятся на 2 вида: сетевые и системные. Сетевые агенты устанавливаются на критичном сегменте сети и обнаруживают атаки путем наблюдения за трафиком (анализируют весь сетевой трафик). Системные агенты устанавливаются на контролируемых узлах и обнаруживают несанкционированную деятельность, осуществляемую на этих узлах (анализируют журналы регистрации операционной системы и деятельность пользователей в режиме реального времени). Агенты также называют сенсорами.

В инсталляции также присутствуют следующие, незначительные для общего описания системы, но важные для обслуживающих систему администраторов, компоненты.

Консоль просмотра событий – предназначена для отображения в реальном времени событий, которые зафиксированы сенсорами.

Из Asset Database передается информация про действующие сенсоры и Event Collector.

Из Event Collector передается в реальном времени информация про зафиксированные сенсорами события для отображения на консоли, а также статус самого Event Collector, Enterprise Database и соединений к сенсорам.

Из Сенсора передается информация про статус сенсора, а также обновления для консоли.

Консоль генерации отчетов – предназначена для генерации отчетов, касающихся событий, зафиксированных сенсорами.

Из Enterprise Database по запросу передается информация про зафиксированные сенсорами события для генерации отчетов.

Asset Database – сохраняет информацию про действующие сенсоры и Event Collector, передает эту информацию по запросу на Консоль просмотра событий и Главную консоль, получает информацию про новые сенсоры и Event Collector от Главной консоли.

Ниже, на рис. 2 приведена «Схема потоков передачи данных» между компонентами системы RealSecure SiteProtector. Она иллюстрирует возможные соединения и направления передачи данных. «Схема направления установления соединения» (рис. 3) иллюстрирует кто является инициатором в установлении соединения между определенными компонентами системы для выполнения функций, которые описаны выше и в соответствии со «Схемой потоков передачи данных».

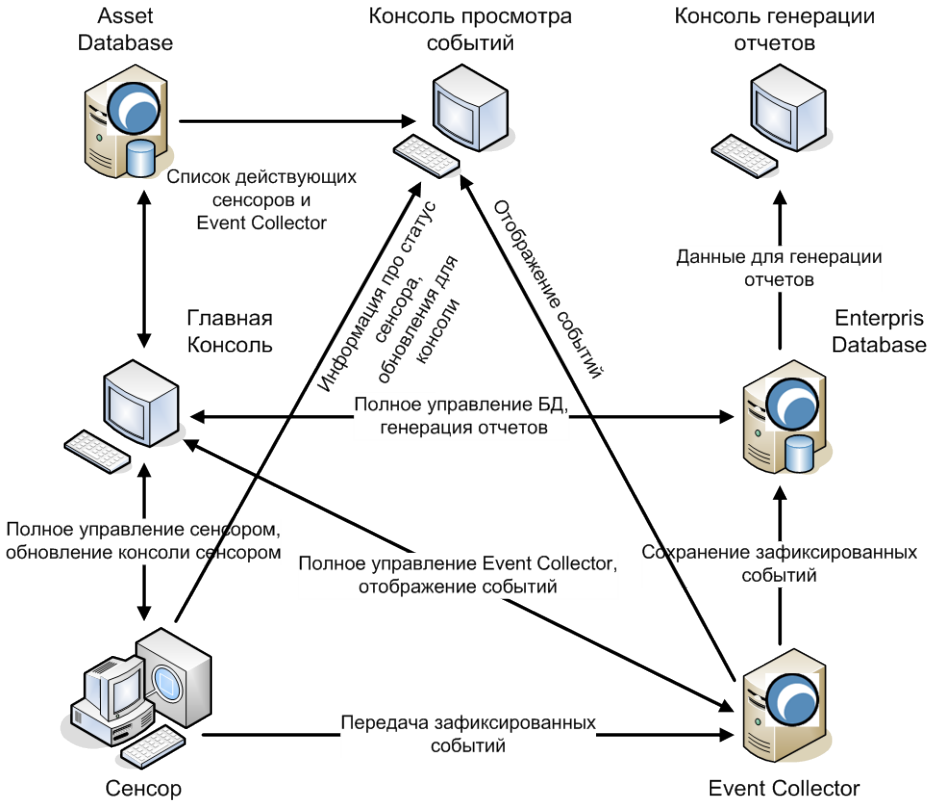

Рисунок 2 – Схема потоков передачи данных

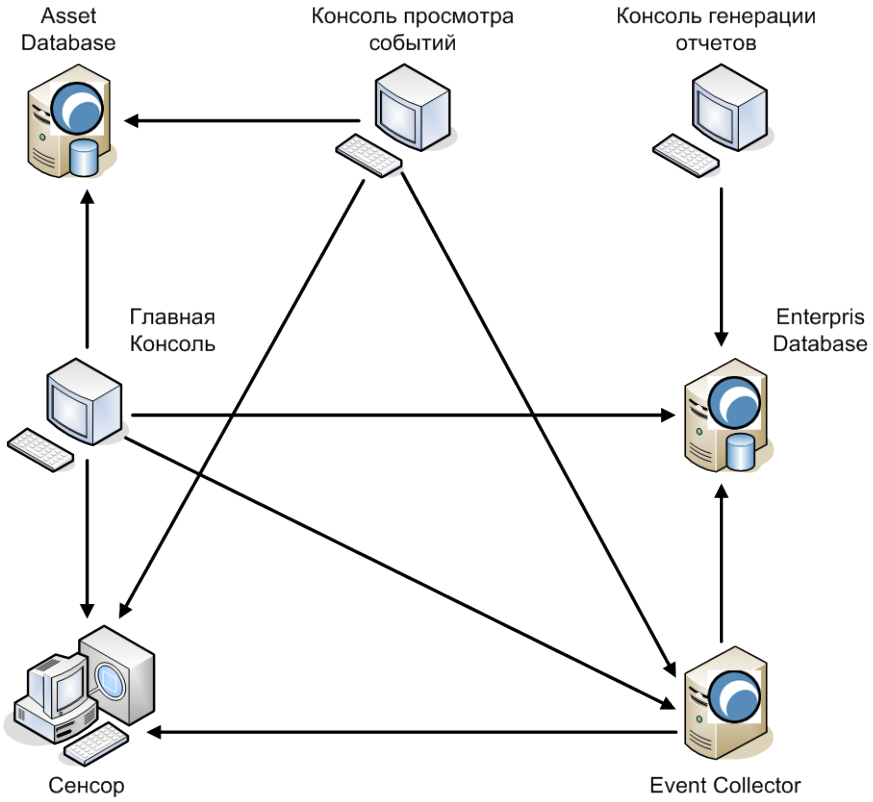

Рисунок 3 – Схема направлений установки соединения

Связь между компонентами системы SiteProtector осуществляется по зашифрованному соединению, исключением является связка Event Collector – MSDE2000SP3, Console – MSDE2000SP3.

Криптопровайдер (определенный комплекс алгоритмов шифрования) выбирается одним и тем же на этапе инсталляции каждого из компонентов системы SiteProtector. При помощи выбранного криптопровайдера автоматически, при инсталляции компонента, генерируется его (компоненты) личная пара ключей открытый/секретный. Для предотвращения возможных утраты/повреждения файла с секретным ключом создается его архивная копия, шифруемая паролем, который вводится во время инсталляции. Эти ключи используются для аутентификации одного компонента системы SiteProtector другим при установлении соединения, а также для защищенного обмена сеансовым ключом шифрования. Сеансовый ключ шифрования используется для шифрования трафика между компонентами системы SiteProtector после установления соединения. Аутентификация одного компонента системы SiteProtector перед другим дает возможность выполняться, так как во время проведения послеинсталляционного конфигурирования (Deployment Wizard) осуществляется обмен открытыми ключами компонент, т. е. на Event Collector передается открытый ключ SiteProtector console, на Server/Network/OS Sensor передаются открытые ключи Event Collector и Console, а на Console передается открытый ключ Event Collector.

В SiteProtector существует возможность задания различных вариантов реагирования на обнаруженные атаки:

- запись факта атаки в регистрационном журнале;
- уведомление об атаке администратора через консоль управления;
- уведомление об атаке администратора по электронной почте;
- аварийное завершение соединения с атакующим узлом;
- запись атаки для дальнейшего воспроизведения атаки;
- реконфигурация межсетевых экранов или маршрутизаторов;
- посылка управляющих SNMP-последовательностей;
- задание собственных обработчиков атак.

Однако SiteProtector, несмотря на достоинства архитектуры, проверенную эффективность в работе во многих государственных и частных учреждениях, является представителем RBID систем со всеми их преимуществами и недостатками. Следует отметить, что типовые недостатки сведены к минимуму и значимым недостатком остается лишь неустойчивость к новейшим типам атак. Если решить эту проблему с помощью методов SBID, то можно получить одно из лучших решений для защиты сети в представляемом SiteProtector сегменте защиты информации, со следующими возможностями:

- большое число распознаваемых атак;
- задание шаблонов фильтрации трафика;
- централизованное управление модулями слежения;
- фильтрация и анализ большого числа сетевых протоколов, в т. ч. TCP, UDP и ICMP;
- фильтрация сетевого трафика по протоколу, портам и IP-адресам отправителя и получателя;
- различные варианты реагирования на атаки;
- аварийное завершение соединения с атакующим узлом;
- управление межсетевыми экранами и маршрутизаторами;
- задание сценариев по обработке атак;
- генерация управляющих SNMP-последовательностей для управления системами HP OpenView(r), IBM NetView(r) и Tivoli TME10(r);
- запись атаки для дальнейшего воспроизведения и анализа;
- поддержка сетевых интерфейсов Ethernet, Fast Ethernet и Token Ring;
- отсутствие требования использования специального аппаратного обеспечения;
- работа с различными Cryptographic Service Provider;
- установление защищенного соединения между компонентами системами, а также другими устройствами;
- наличие всеобъемлющей базы данных по всем обнаруживаемым атакам;
- отсутствие снижения производительности сети;
- работа с одним модулем слежения с нескольких консолей управления;
- мощная система генерация отчетов;
- использование протокола ODBC;
- различные форматы отчетов;
- мощная система подсказки;
- простота использования и интуитивно понятный графический интерфейс;
- невысокие системные требования к программному и аппаратному обеспечению.

Таким образом, мощные возможности анализа, реализованные в системе RealSecure SiteProtector, позволяют ответить на интересующие любого администратора безопасности вопросы:

- текущее состояние безопасности;
- статистические данные по злоумышленникам, атакам и уязвимостям в организации;
- ресурсы, часто подвергающиеся атаке или находящиеся под действием атаки в данный момент;
- наиболее уязвимые узлы корпоративной сети;
- скоординированные атаки;
- успешные атаки злоумышленников.

Система SiteProtector позволяет отслеживать злоумышленников в реальном режиме времени, что является незаменимым механизмом для сбора доказательств несанкционированной деятельности.

Расширенная система разграничения доступа позволяет разделить обязанности по управлению и контролю различных компонентов системы SiteProtector. Например, администратор безопасности может конфигурировать систему SiteProtector и управляемые ею компоненты (RealSecure, Internet Scanner и т. д.), оператор - отслеживать события от этих компонентов в реальном режиме времени, а аналитики - создавать отчеты и анализировать собранные данные.

Система SiteProtector автоматизирует процесс удаленной инсталляции компонентов, входящих в семейство SiteProtector, что приводит к существенному облегчению труда администратора и повышает масштабируемость решений компании ISS. Данный механизм реализуется за счет технологии Package Installation Manager, которая позволяет устанавливать на удаленные узлы сенсоры SiteProtector и агенты System Scanner без присутствия администратора.

База данных сигнатур, уязвимостей и других обнаруживаемых событий системы SiteProtector содержит подробную информацию о каждом из них, включая:

- пошаговые рекомендации по устранению возможности их реализации и использования;

- подверженных атаке или уязвимости операционных системах и приложениях;
- примеры ложных срабатываний;
- дополнительные ссылки на патчи и обновления, устраняющие данные проблемы и т. д.

Література: ***1.*** *Голяка А. Таксономия, тенденции развития систем обнаружения вторжений. «Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні»* ***2.*** *http://www.iss.net/.* ***3.*** *Петренко С. А., Петренко А. А. Аудит безопасности Intranet. ДМК Пресс, 2002.* ***4.*** *Сопроводительная документация к программному продукту Site Protector.*

УДК 004.4

ВОЗМОЖНОСТИ ПРИМЕНЕНИЯ МЕТОДОВ ИНТЕЛЛЕКТУАЛЬНОГО АНАЛИЗА ДАННЫХ В СИСТЕМАХ ОБНАРУЖЕНИЯ ВТОРЖЕНИЙ

Александр Голяка
НБУ

Аннотация: **Представлена возможность применения методов интеллектуального анализа данных в системах обнаружения атак.**
Summary: **Possibility application of Data Mining methods in the intrusion detection systems is presented.**
Ключевые слова: **Системы обнаружения вторжений, Data Mining, метод опорных векторов.**

Несмотря на то, что симбиоз RBID и SBID систем [1] повышает возможности обнаружения атак, однако, описанных в статье [1, 2] проблем SBID систем это не решает. Главной и принципиальной проблемой SBID систем являются либо ошибки первого, либо второго рода в терминах математической статистики, в зависимости от выставленного порогового значения для сигнализации атаки. В связи с этим, очевидна недостаточность хорошо изученного аппарата статистических моделей при построении SBID систем. В настоящее время ищутся новые методы анализа данных в системах обнаружения вторжений (СОВ) и все больше внимания уделяется применению методов интеллектуального анализа данных (ИАД, Data Mining). ИАД – это процесс выявления значимых корреляций, образцов и тенденций в больших объемах данных. Встречаются такие определения термина Data Mining:

- это процесс выделения из данных неявной и неструктурированной информации и представления ее в виде, пригодном для использования;

- это процесс обнаружения в сырых данных ранее неизвестных, нетривиальных, практически полезных и доступных, интерпретации знаний, необходимых для принятия решений в различных сферах человеческой деятельности.

К методам и алгоритмам Data Mining относятся следующие: искусственные нейронные сети, деревья решений, символьные правила, методы ближайшего соседа и k-ближайшего соседа, метод опорных векторов, байесовские сети, линейная регрессия, корреляционно-регрессионный анализ; иерархические методы кластерного анализа, неиерархические методы кластерного анализа, в том числе алгоритмы k-средних и k-медианы, методы поиска ассоциативных правил, в том числе алгоритм Apriori, метод ограниченного перебора, эволюционное программирование и генетические алгоритмы, разнообразные методы визуализации данных и множество других методов.

Data Mining может состоять из трех стадий.

1. Выявление закономерностей (осуществляется исследование набора данных с целью поиска скрытых закономерностей; также должна осуществляться валидация закономерностей, т. е. проверка их достоверности на части данных, которые не принимали участие в формировании закономерностей);
2. Использование выявленных закономерностей для предсказания неизвестных значений (обнаруженные закономерности используются непосредственно для прогнозирования – решаются задачи классификации и прогнозирования);
3. Анализ исключений; стадия предназначена для выявления и объяснения аномалий, найденных в закономерностях (анализируются исключения или аномалии, выявленные в найденных закономерностях).

Методы Data Mining

Статистические методы Data Mining классифицированы на четыре группы: