ЦЕНТРАЛИЗОВАННОЕ УПРАВЛЕНИЕ СИСТЕМАМИ БЕЗОПАСНОСТИ

Централизованная система управления средствами защиты позволяет существенно повысить эффективность работы отдела ИБ. Как лучше организовать такую систему?

Сегодня набор средств защиты, установленный в сети организации средних и больших размеров, достаточно разнообразен: системы сетевой защиты (межсетевые экраны, системы обнаружения и предотвращения вторжений, криптографическая защита каналов связи), антивирусные решения и системы защиты от спама, комплексы предотвращения утечек (DLP) и другие средства защиты.

Все эти решения по обеспечению информационной безопасности нуждаются в средствах централизованного управления. Управлять настройками средств защиты даже на нескольких десятках рабочих станций крайне проблематично.

В связи с этим сейчас большинство разработчиков включает в состав своих решений приложения для централизованного управления. Как правило, это веб-консоль или клиентское ПО, устанавливаемое на рабочее место администратора безопасности. С помощью данного приложения можно устанавливать клиенское ПО на машины пользователей, изменять настройки, обновлять и удалять агентов.

Какова экономическая эффективность централизации управления? При обслуживании большого парка машин – более сотни – постоянно возникают различные проблемы на рабочих местах пользователей. И если у компании есть филиальная сеть, то сопровождение удаленных рабочих мест становится серьезной проблемой, требующей наличия в штате нескольких специалистов, основной задачей которых будет ездить на площадки и на месте решать возникающие проблемы. Конечно, сейчас для этого часто используют средства удаленного администрирования, например, Remote Admin, но при отсутствии средств централизованного управления обслуживание рабочих мест также потребует значительных затрат. Поэтому при проектировании внедрения какой-либо системы защиты крайне важно уделить внимание наличию средств централизованного управления. Это поможет сэкономить при дальнейшем сопровождении.

У всех свое окно

Централизованная консоль – это удобно. Но есть одна проблема: у каждого программного продукта такое средство управления свое. Так, консоль для антивируса Касперского не подойдет для управления Доктор Веб. А система управления для оборудования Cisco не сможет работать с Huawei или Juniper.

Традиционный выход, который предлагают разработчики, – это покупать несколько средств защиты у одного производителя, тогда в одном приложении можно будет работать сразу со всеми приобретенными средствами. Однако есть ряд недостатков, о которых стоит поговорить.

Во-первых, решениями одного вендора практически невозможно покрыть все направления защиты информации. Вряд ли можно найти производителя, который выпускал бы и сетевое оборудование, и антивирусы, и DLP, и средства однократной аутентификации.

Хотя большинство крупных игроков идет по пути укрупнения своего бизнеса, скупая перспективные маленькие компании, тем не менее пока покрыть весь спектр никому не удалось.

Во-вторых, решение от одного разработчика – это не очень хорошо с точки зрения безопасности. Так, неустраненная уязвимость в продуктах одного вендора может привести к захвату всей инфраструктуры безопасности на предприятии.

И, в-третьих, зачастую набор средств защиты от одного именитого производителя может обойтись существенно дороже (и не всегда они лучше), чем «самостоятельная» закупка аналогичных средств у других разработчиков.

В связи с вышеизложенным возникает необходимость в некотором наборе приложений для управления средствами информационной безопасности на предприятии.

Помимо средств защиты, о которых речь шла выше, не стоит также забывать и об управлении средствами информационной безопасности, встроенными в операционную систему и основные приложения, такие как базы данных, веб-серверы, офисные пакеты и другие. Здесь нам также потребуется единая консоль администрирования.

Итак, мы приходим к множеству окон управления на компьютере администратора безопасности. Совершенно очевидно, что работа одновременно за несколькими консолями не слишком эффективна, так как нельзя постоянно следить за несколькими окнами. Поэтому необходимо правильно сгруппировать средства защиты, чтобы работа с ними была удобной.

Распределяем функционал

Для этого нам необходимо правильно определить и сгруппировать все те функции, которые содержит система централизованного управления. Прежде всего, как упоминалось выше, выполнение задач по развертыванию и администрированию клиентского программного обеспечения, настроек и политик.

Что это такое? Установка клиентов. Если, к примеру, мы разворачиваем новый корпоративный антивирус, то нам необходимо установить его клиентов на все компьютеры в сети. Затем необходимо распространить политики (какие файлы сканировать, когда обновляться, когда производить полную проверку), далее необходимо следить за состоянием системы защиты (на скольких компьютерах не прошло обновление баз, где клиенты неактивны и т.д.).

Каков типичный набор средств защиты информации для корпоративной сети средних и больших размеров? Основу составляют следующие подсистемы:

- подсистема антивирусной защиты;
- подсистема резервного копирования и архивирования;
- подсистема обнаружения атак;
- подсистема централизованного мониторинга и аудита событий ИБ;
- подсистема межсетевого экранирования;
- подсистема защиты каналов передачи данных;
- подсистема управления доступом (идентификации и аутентификации пользователей);
- подсистема предотвращения утечек информации.

Сгруппируем их следующим образом.

Сетевые средства защиты:

- подсистема межсетевого экранирования;
- подсистема защиты каналов передачи данных;
- подсистема обнаружения атак;

Прикладные средства защиты:

- подсистема антивирусной защиты;
- подсистема предотвращения утечек информации;
- подсистема резервного копирования и архивирования;
- подсистема управления доступом (идентификации и аутентификации пользователей);

Мониторинг:

- подсистема централизованного мониторинга и аудита событий ИБ.

Рисунок 1. Группы подсистем средств защиты информации для корпоративной сети

Сеть в одном окне

С первой группой все достаточно просто. Многие разработчики сетевого оборудования и средств защиты предлагают свои решения под управлением единой консоли управления. Например, решение от Cisco для централизованного управления, мониторинга и аудита – Cisco Security Manager (CSM), входящее в состав Cisco Security Management Suite. Это приложение позволяет осуществлять управление и мониторинг сетевых средств защиты, таких как межсетевые экраны, средства обнаружения атак и защиты каналов связи. Важно, что такие системы могут применяться не только для сетевых устройств Cisco, но также по всей вертикали информатизации предприятия на уровне операционных систем и приложений.

Средства событийного протоколирования, мониторинга и аудита также хорошо представлены в целом ряде продуктов Cisco. Они позволяют вести мониторинг сети в реальном времени,

распределять и структурировать событийную информацию, производить событийный аудит, в том числе с использованием развитых средств событийной корреляции и составлять ясные, структурированные отчеты.
Кроме собственно решений Cisco Systems, CSM позволяет управлять также криптосредствами S-Terra. Это российский разработчик средств криптографической защиты, чьи решения соответствуют всем требованиям российских регуляторов и поэтому активно используются в России для защиты персональных данных.
Еще одним интересным инструментом централизованного управления средствами сетевой безопасности является решение Stonegate Management Console (SMC), предназначенное для управления продуктами McAfee (Stonesoft). SMC дает возможность проводить централизованный мониторинг и генерацию разнообразных отчетов о событиях в сети. Решение StoneGate предлагает централизованное средство управления, позволяющее управлять межсетевыми экранами, криптомаршрутизаторами Stonegate FW/VPN и системами предотвращения вторжений Stonegate IPS. SMC – это программное обеспечение, устанавливаемое на физический или виртуальный сервер.
Завершая тему сетевых средств защиты, следует также упомянуть решения «Кода Безопасности» – Континент Центр Управления Сетью. Континент ЦУС – это устройство, предназначенное для управления криптошлюзами (которые часто используют и как межсетевые экраны), а также решениями Континент ДА, которые предназначены для обнаружения атак. ЦУС позволяет осуществлять централизованное распространение настроек для всех подключенных устройств.
Стоит отметить, что Cisco CSM не является обязательным компонентом для управления устройствами Cisco, то есть администрировать их можно напрямую, посредством командной строки или веб-интерфейса. А вот SMC и ЦУС являются обязательными компонентами. Без них управлять средствами защиты не получится.

Прикладная защита

Перейдем к прикладным средствам защиты. Здесь все уже не так красиво, так как обойтись одним окном управления не получится. Так, например, для управления антивирусными продуктами «Лаборатории Касперского» требуется свое средство управления – Kaspersky Administration Kit. Оно предлагает расширенные возможности управления продуктами «Лаборатории Касперского», установленными на рабочих станциях и файловых серверах Windows: контроль рабочих мест, гибкие настройки работы защитных решений (в том числе в виртуальных средах) и так далее.
Аналогично и для работы со средствами резервного копирования или DLP также требуется своя консоль.

Всевидящее око

Итак, мы разобрались с системами управления защиты различных прикладных компонентов. У нас все равно получается несколько консолей, с которыми необходимо работать, но все они нужны только в ситуациях, когда необходимо выполнить какие-либо административные задачи. Но самой рутинной задачей, требующей постоянного внимания, является мониторинг. Этот процесс важен для любой системы, однако для средств обеспечения информационной безопасности он наиболее критичен, ведь, если мы пропустим атаку, это может привести к весьма печальным последствиям. Осуществлять мониторинг в каждой из консолей управления, мягко говоря, неудобно. Поэтому здесь наилучшим решением будет использование единой системы централизованного управления событиями информационной безопасности (SIEM). Данная система осуществляет сбор наиболее важных событий со всех систем управления средствами защиты. Например, с межсетевых экранов собирается информация об обнаруженных сетевых атаках, таких как сканирование портов. С систем обнаружения вторжений приходят события о подозрительном трафике с определенных узлов. С антивирусной системы собираются события о вирусных инцидентах. Также весьма полезно знать, на каких рабочих станциях давно не обновлялись антивирусные базы. С системы DLP приходят события об инцидентах утечки информации с обязательным указанием имени пользователя.
Сбор событий с целевых источников осуществляется посредством следующих протоколов:

- **Syslog** (протокол событийного протоколирования, общий для семейства ОС Unix и большинства сетевых устройств). Syslog позволяет передавать отдельные события (например, формировать тревожное сообщение), защищать систему аудита безопасности, разделяя полномочия доступа к операционному управлению и к системам событийного протоколирования;

- **SNMP** (протокол сетевого управления), обеспечивающий контроль состояния устройств защиты и мониторинг событий в реальном времени;
- **ODBC** – позволяет собирать события из таблиц в базах данных;
- **текстовые файлы** – коннекторы SIEM собирают события, непосредственно подключаясь к файловым ресурсам и собирая текстовые записи из файлов;
- **Windows Event Log** – сбор событий Windows.

Поговорим также о том, какие основные SIEM-решения предлагаются на рынке.

Система SIEM состоит из следующих основных компонентов:

- **ядро системы** – в нем производится проверка на соответствие событий правилам корелляции, а также построение отчета;
- **база данных** – в ней хранятся полученные события;
- **коннекторы** – эти компоненты отвечают за сбор событий непосредственно с источников.

HP ArcSight

Начнем с HP ArcSight. Платформа ArcSight ESM обеспечивает взаимосвязанную инфраструктуру, способную определить каждое событие, поместив его в рамки контекста того, кем или чем оно вызвано, где, когда и почему произошло, а также каково его влияние на бизнес-риски. Решение реализует логику, позволяющую соотнести такие общие идентификаторы, как адреса электронной почты, логины и учетные записи и составить отчеты обо всех действиях, произведенных пользователем в рамках системы, с помощью приложений, учетных записей и IP-адресов. Существуют как программно-аппаратные, так и чисто программные варианты реализации решения.

QRadar

Еще одним популярным SIEM-решением является QRadar. Этот продукт позволяет эффективно обеспечить безопасность сети и критически важных корпоративных ресурсов в корпоративной ИТ-инфраструктуре. Решение представляет собой аппаратный модуль, на котором размещаются все компоненты SIEM.

RSA

RSA Security Analytics несколько отличается от классических SIEM-решений, описанных ранее. Фактически этот продукт является комбинацией технологии SIEM и технологии мониторинга угроз безопасности в сетевом трафике при его анализе на 2-7 уровнях модели OSI. При этом механизмы, реализующие эти технологии, заимствованы из продуктов RSA enVision и RSA NetWitness. Эти механизмы были объединены в интегрированную, функциональную и высокопроизводительную систему, дополненную специализированным хранилищем данных RSA Security Analytics Warehouse и информационным сервисом RSA Live Intelligence. Это решение также представляет собой программно-аппаратные модули. При этом компоненты архитектуры можно разнести на отдельные устройства, что позволяет увеличить масштабируемость системы в целом.

Для наибольшей эффективности работы с SIEM-системой рекомендуется выводить ее рабочее окно, в котором отражаются все инциденты, на большую плазменную панель, размещенную на стене комнаты, где работают администраторы по безопасности. Это заметно увеличит эффективность мониторинга, так как появление инцидентов с высокой (красной) критичностью сразу заметят все сотрудники.

Вывод

Система управления состоит из нескольких модулей, каждый из которых используется по мере необходимости, но основной модуль – мониторинг, на который стекаются все события об инцидентах ИБ, должен постоянно просматриваться ответственными специалистами. Такой подход к обеспечению централизованного управления позволит оптимизировать работу отдела информационной безопасности и снизить операционные расходы на поддержку средств безопасности.

Источник
Выпуск №1 (44) / Централизованное управление системами безопасности
http://bit.samag.ru
АНДРЕЙ БИРЮКОВ, системный архитектор (автор статьи)