Н. Г. Милославская, А. И. Толстой

МОНИТОРИНГ СЕТЕВОЙ БЕЗОПАСНОСТИ С ПРИМЕНЕНИЕМ КОММУТАТОРОВ[1]

Введение

Сетевая среда организаций продолжает разрастаться и усложняться. При этом существенно возрастает ценность активов, находящихся в этой среде, и зависимость всего бизнеса организации от их защищенности (в общепринятом смысле поддержания свойств конфиденциальности, целостности, доступности и дополнительных аутентичности, неотказуемости, учетности и надежности). Для постоянного владения ситуацией в отношении обеспечения информационной безопасности (ОИБ) в сети организации необходимо контролировать этот процесс. Наряду с аудитом ИБ справедливо выделяют такой вид проверки состояния ИБ, как мониторинг, осуществляемый силами специалистов организации на постоянной основе. По результатам мониторинга ИБ руководство организации должно принимать обоснованные решения, касающиеся стратегических и тактических улучшений в ее сетевой среде. Качество принимаемых решений напрямую зависит и от результатов, полученных во время мониторинга. Только современные, производительные, достаточно просто управляемые средства мониторинга могут предоставить всю необходимую для этого информацию.

1. Роль мониторинга в управлении информационной безопасностью

Управление ИБ — неотъемлемая часть управления любой современной организацией в целом, независимо от ее размера и сферы деятельности. Управление ИБ представляет собой сложный непрерывный процесс, перед которым стоит множество целей и задач, являющихся обеспечивающими, вспомогательными по отношению к основным бизнес-целям и задачам организации. Для успешного управления ИБ должна быть создана учитывающая специфику организации и адекватная ее требованиям в отношении ОИБ система управления информационной безопасностью (СУИБ). Функционирование данной системы адекватно описывается с помощью циклической модели улучшения процессов — цикла PDCA (от англ. Plan-Do-Check-Act — «планируй — выполняй — проверяй — действуй»). Важнейший этап цикла — проверка ОИБ в организации, основная цель которой — оценить текущее состояние ОИБ, а также адекватность ОИБ поставленным целям и задачам бизнеса. Результаты качественно выполненной проверки позволяют построить оптимальную по эффективности и результативности корпоративную систему защиты, адекватную ее текущим задачам и целям бизнеса.

Одним из ключевых элементов управления ИБ является мониторинг ИБ, под которым понимается постоянное (непрерывное) наблюдение за регистрируемыми событиями, влияющими на ОИБ организации в конкретной среде (системе, сети, сервисе), а также сбор, анализ и обобщение результатов наблюдений [1]. Мониторинг ИБ реализуется на базе контроля за соблюдением базовых требований по ОИБ и предписанных регламентов (контроль штатности режима функционирования этой среды). Деятельность по мониторингу сетевой безопасности (МСБ) — мониторингу ИБ в сетевой среде организации — является неотъемлемой частью деятельности по мониторингу ИБ организации.

2. Цели и процессы мониторинга сетевой безопасности

Среди основных целей МСБ можно выделить следующие:

1) контроль за реализацией в организации положений внутренних и внешних документов по ОИБ для обнаружения отклонений от принятых требований бизнеса и требований по ОИБ (например, зафиксированных в политике в отношении логического доступа к информационным активам);

[1] Данная работа выполнена в НИЯУ МИФИ при финансовой поддержке Министерства образования и науки Российской Федерации в рамках проекта «Создание инженерно-технических решений для высокотехнологичного производства инновационных программно-аппаратных средств защиты информации на базе перспективных высокоскоростных интерфейсов информационного взаимодействия», выполняемого совместно ООО «ОКБ САПР».

2) контроль качества (под которым будем понимать в данном случае результативность и эффективность) используемых защитных мер;

3) выявление нештатных, в том числе злоумышленных, действий с информационными активами и бизнес-процессами организации;

4) выявление событий ИБ, часть из которых в дальнейшем классифицируется как инциденты ИБ;

5) выявление уязвимостей активов, которыми могут воспользоваться злоумышленники для реализации атак на системы, сети и сервисы как самой организации, так и ее бизнес-партнеров или пользователей общедоступных сетей типа Интернета;

6) обеспечение доказательной базы на случай расследования компьютерных преступлений.

Процессы МСБ в рамках процесса управления ИБ включают в себя следующую деятельность:

1) поиск, отслеживание, наблюдение, накопление, систематизация, оценивание сведений, относящихся к области ОИБ;

2) прогнозирование состояния и качества всех объектов и процессов в информационной среде организации.

Подчеркивая контролирующие функции МСБ, следует отметить, что его техническим аспектам свойственна иерархичность, предполагающая необходимость наличия контролирующих механизмов на всех уровнях контроля — физическом, сетевом, операционных систем, прикладном. МСБ должен осуществляться для различных элементов среды организации — ИС, ПО, устройств, конфигураций, электронной почты, связи с Интернетом, парольной защиты и т. п.

3. Трудности осуществления мониторинга сетевой безопасности в современных сетях

Во многом результаты МСБ зависят от качества и полноты базовых настроек и механизмов регистрации событий ИБ и собранной на этой основе информации, которая, в свою очередь, влияет на дальнейшую обработку рисков ИБ и принятие решений по соответствующим рискам защитным мерам.

Почему же МСБ трудно реализуем в современных сложных сетевых средах? В общем и целом сети продолжают расти. Приложения и предоставляемые пользователям сервисы становятся все более важными для бизнеса. Объем трафика постоянно возрастает. Атаки на все сетевые ресурсы осуществляются довольно часто и постоянно, и нацелены они на несколько точек внутри сети, а не только на ее периметр. В связи с этим инфраструктура МСБ, обеспечивающая данный процесс, с большим набором средств мониторинга становится все более сложной, ресурсоемкой и замедляющей производительную работу сети.

Можно выделить три основные проблемы, усложняющие МСБ.

Во-первых, ограниченность применяемых в сетях таких средств, как SPAN-порты и ответвители TAP, которые затрудняют для средства мониторинга доступ и визуализацию всего трафика, за которым они должны следить, — будь то выявление уязвимостей или характерных признаков штатного исполнения приложений, отклонение от которых является событием ИБ. В такой ситуации специалисты по сетевой безопасности теряют часть важной информации из тех сегментов сети, которые были определены как менее приоритетные для контроля.

Напомним, что TAP (контрольная точка доступа) представляет собой пассивное средство расщепления (или ответвления), установленное между представляющим интерес конкретным устройством и сетью. Оно передает встречные потоки дуплексного трафика (как отправленные, так и полученные потоки данных) одновременно на отдельные выделенные каналы, гарантируя поступление всех данных на средство мониторинга в режиме реального времени.

Большинство коммутаторов копируют активность одного или более портов через SPAN-порт (Switch Port Analyzer — анализатор портов коммутатора), также известный как зеркальный порт. Зеркалирование портов (в этом значении для продуктов разных производителей кроме названного термина еще встречаются «Port mirroring» и «Roving analysis port» (RAP)) используется на сетевом коммутаторе для посылки копий всех сетевых пакетов, видимых на одном порте (или нескольких портах) коммутатора, для мониторинга сетевого соединения на другом порте коммутатора, что обычно используется в системах обнаружения вторжений. К SPAN-порту можно добавить устройство анализа. Но при перегрузке SPAN-порта пакеты отбрасываются, слишком короткие и длинные пакеты, как и дефектные пакеты с ошибками, не захватываются из-за соответствующей фильтрации.

На выбор одного из этих подходов влияют два важных фактора: тип анализа и пропускная способность канала. SPAN-порт хорошо работает в мало загруженной сети или когда анализ не зависит от отброшенных пакетов (плюс возможность мониторинга внутреннего трафика коммутатора). TAP идеально подходит, когда анализ требует полной видимости всего трафика, в том числе ошибок физического уровня, и если нагрузка на сеть варьируется от умеренной до высокой.

В качестве эффективного компромисса между TAP и SPAN-портом используется так называемый TAP-агрегатор, или агрегатор каналов, обладающий некоторыми достоинствами TAP и не имеющий недостатков SPAN-порта (в частности, TAP-агрегатор снимает с центрального процессора коммутатора нагрузку по копированию всех данных, проходящих через порты; также он может изменять время взаимодействия фреймов, изменяя время отклика, и задает приоритет для данных SPAN-порта ниже, чем для обычных данных «порт — порт»). Это устройство объединяет трафик, ответвляемый из нескольких контролируемых каналов, и выводит суммарный поток через свои порты мониторинга.

Во-вторых, не имея возможности визуализировать весь сетевой трафик, нельзя ожидать четкого, обоснованного понимания всего происходящего в сети и, следовательно, качественного контроля трафика. А без этого можно работать только в режиме реагирования, а не проактивно пресекать любую несанкционированную деятельность.

В-третьих, без полной прозрачности сети не получится оптимизировать производительность применяемых средств мониторинга — они будут использоваться как придется. И, возможно, специалист по сетевой безопасности через некоторое время потребует приобрести дополнительно еще и новые средства.

Следствием вышеперечисленного является то, что монитор использования сети предоставляет частичную видимость, система обнаружения вторжений защищает лишь от конечного числа атак, монитор производительности приложений перегружен, а регистратор данных о событиях в сетевой среде переполнен.

4. Современный подход к реализации мониторинга сетевой безопасности с использованием коммутаторов

Технологические достижения последних двух десятилетий способствуют тому, чтобы каждодневный МСБ упростился. Теперь специалистам по сетевой безопасности не нужно каждый день вручную дублировать пакеты, создавать и использовать большое количество специально написанных сценариев, интуитивно фильтровать и изменять маршруты трафика. Веских причин, по которым они должны выполнять рутинные операции с использованием программ, имеющих командную строку прошлого поколения, больше не осталось. Требованием времени является МСБ, по простоте приближающийся к пользованию сервисами Google или работе с современными клиентскими приложениями.

Решить указанные выше проблемы можно, используя так называемые коммутаторы мониторинга сетевой безопасности (КМСБ) [2, 3].

Сделаем короткое отступление о коммутаторах (англ. switch). Они в сети, наравне с концентраторами (англ. hub), являются центральными точками подключения компьютеров и других сетевых устройств, но в отличие от концентраторов анализируют все пакеты по мере их поступления, проверяют MAC-адреса источника и назначения и передают пакет на нужный порт. Многие коммутаторы могут быть сконфигурированы так, чтобы переправлять пакеты на специальный порт для мониторинга. Коммутаторы известны высокой производительностью и защищенностью, поскольку они переправляют пакеты только в один порт, тем самым снижая риск несанкционированного мониторинга.

КМСБ существенно снижают нагрузку на сеть и позволяют контролировать функционирование используемых в сети средств мониторинга, фактически централизуя их работу, а также обеспечивают интеллектуальную автоматизацию и даже некоторые функции передовых графических пользовательских интерфейсов, значительно упрощая работу по выявлению аномального, нештатного поведения всех сетевых ресурсов. Они предоставляют больший контроль над сетью и создают условия для более производительной работы используемых средств мониторинга.

При использовании КМСБ мониторинг становится похожим по виду и осуществлению, с точки зрения специалиста, на работу с клиентскими приложениями, но с надежными возможностями, предъявляемыми к инфраструктуре МСБ. Путем переноса общих, низкоуровневых, выполняемых вручную задач со средств МСБ на коммутаторы последние позволяют специалистам по сетевой безопасности качественнее выполнять возложенную на них работу (здесь вполне уместна аналогия с Excel-таблицами, автоматически выполняющими некоторые вычисления и вносящими исправления).

5. Преимущества использования коммутаторов мониторинга сетевой безопасности в сетевой среде организации

КМСБ предоставили такие возможности, которые произвели революцию в клиентских приложениях:

- КМСБ используют интеллектуальные технологии автоматизации, что обеспечивает простое и наглядное управление: для повседневной работы интерфейс командной строки заменен на графический интерфейс, использующий принцип «подведи курсор и нажми» (от англ. point-and-click interface). Также возможен просмотр работы нескольких средств мониторинга в одном окне. (Конечно, можно и нужно сохранить командную строку, чтобы в случае необходимости писать специальные скрипты или решать случающиеся время от времени скрытые проблемы.);
- КМСБ заменяют неудобные, в основном ручные и совмещенные с фильтрацией трафика, методы на динамическую фильтрацию — более простую, почти не требующую усилий;
- КМСБ заменяют выполняемые вручную действия интеллектуальной, без ручного вмешательства автоматизацией важнейших задач управления, что повышает гибкость управления без приобретения дополнительных навыков или увеличения персонала;
- некоторые производители КМСБ ориентированы на уже имеющиеся в организациях средства МСБ для автоматизации выполняемых с их помощью основных трудоемких задач. Автоматизация предвосхищает и высвечивает проблемы прежде, чем они будут обнаружены, а это позволят быть проактивными, а не реактивными. Это похоже на автозамену в офисных приложениях Microsoft.

Существенное упрощение МСБ предоставляет организациям следующие преимущества, которые позволяют им осуществлять их бизнес быстрее и эффективнее, с большей уверенностью:

- можно достичь нового уровня эффективности, гибкости и масштабируемости;
- можно избежать распространенных ИТ-проблем и меньше пострадать от простоев;
- можно управлять большими объемами трафика в более сложных, сильно распределенных сетях при помощи имеющихся средств МСБ, используя навыки персонала.

КМСБ обеспечивает полную прозрачность сети с точки зрения видимости, управления и производительности. Это значительно упрощает управление сетевым трафиком и средствами МСБ, потому что легко видеть все, что происходит в сети.

1. Видимость. Все средства МСБ имеют доступ ко всем данным в нескольких сегментах сети и полную картину сетевого трафика. Каждое средство может иметь копию данных из одного или нескольких сегментов. Таким образом больше средств могут иметь доступ к одной и той же сети.

Практически без усилий можно видеть, куда идет трафик, как фильтруются пакеты, балансировку нагрузки, агрегирование пакетов от одного и того же источника, отправку пакетов от одного и того же источника двум разным получателям, репликацию и множественную посылку пакетов и т. д.

Возникающие в сети проблемы выявляются гораздо проще, поэтому специалист по сетевой безопасности больше времени может посвятить анализу сетевого трафика, а не охоте за ним (его преследованию).

2. Управление. Все действия производятся непосредственно в потоке данных, предоставляя нужную информацию нужным средствам в нужное время. Тогда можно реагировать на изменения, возникновение проблем и открывающиеся возможности быстрее и с большей точностью. Интеллектуальные автоматизированные методы управления позволяют делать больше и качественнее с меньшими усилиями. Например:

- интеллектуальное распределение трафика: агрегирование пакетов при нехватке SPAN/TAP, маршрутизация пакетов в соответствующие точки, снижение скорости передачи сетевого трафика и пр., что позволяет использовать рассчитанные на 1 или 10 Гбит/с средства для мониторинга сетей с пропускной способностью 10 или 40 Гбит/с;
- обработка пакетов: фильтрация, очистка, «нарезка» (фрагментация); репликация и множественная посылка пакетов; распределение нагрузки между несколькими средствами; буферизация трафика в моменты пиковой нагрузки и т. д.;
- адаптивный отклик: проактивный мониторинг изменений, пропускной способности, уязвимостей, инцидентов и атак; автоматическая регулировка доставки пакетов, соответствующая текущим потребностям; динамическое обновление конфигураций без длительного предварительного утверждения или ручного вмешательства; значительное улучшение и упрощение поиска и устранения неисправностей.

Так, КМСБ при совместном использовании с SIEM-системой (системой управления событиями ИБ [4]) будет автоматически захватывать пакеты и связывать само наличие этих пакетов или их содержимое с событиями ИБ, идентифицируемыми SIEM-системой, ускоряя ответные действия и сбор доказательств для последующего расследования. Предпринимаемые действия в основном будут проактивными, а не реактивными: таким образом можно быстро отразить зарождающуюся атаку злоумышленников или выполнить компьютерно-техническую экспертизу для внесения соответствующих изменений в архитектуру сети. Специалисты по сетям и безопасности могут просматривать одни и те же сетевые данные и более эффективно сотрудничать в решении или предотвращении проблем.

3. Производительность. В результате автоматического перераспределения нагрузки, что важно, но не столь критично для отдельных средств МСБ, возрастает производительность используемого сетевого оборудования и снижается потребность в приобретении дополнительного. Например, распределенная фильтрации пакетов, балансировка нагрузки, дублирование пакетов, их очистка, фрагментация и установка меток могут дать значительную экономию средств. Появляется возможность управлять тем же или большим трафиком при использовании меньшего количества средств, а также решить проблему нехватки SPAN/TAP. Часть средств МСБ освободится для решения непосредственно тех задач, для которых они разрабатывались, что повысит

производительность каждого из этих средств. Интеллектуальная фильтрация и автоматизация упрощают все это, обеспечивая динамическое выравнивание нагрузки с сохранением целостности потоков и предварительной фильтрацией трафика с использованием функции глубокого анализа пакетов (англ. deep packet inspection, BDPI) [3].

Использование КМСБ в сети организации имеет и ряд других важных преимуществ.

КМСБ позволяет опережать рост и изменения сетей, работая с имеющейся инфраструктурой и применяемыми в текущий момент средствами МСБ. Они агрегируют, фильтруют и реплицируют трафик таким образом, что все средства получают необходимые данные в нужное время. Как результат — более простое, легкое и понятное восприятие поведения сети, включая поведение пользователей, уязвимости, пропускную способность, работу приложений и отказоустойчивость ИТ-инфраструктуры.

Такое решение равносильно получению требуемой пропускной способности за счет устранения недостаточного и чрезмерного использования. Это позволит идти в ногу с растущими требованиями мониторинга, порожденными в том числе массовым спросом со стороны мобильных пользователей.

КМСБ легко интегрируется и с себе подобными средствами, и с теми продуктами, которые уже есть на рынке. Они просты в развертывании, настройке и использовании. Панель управления КМСБ, использующая известные подходы «подведи курсор и нажми» или «перетащи и оставь», упрощает все выполняемые действия.

КМСБ разработаны и для того, чтобы было легче применять соответствующие размерам сети средства МСБ (1, 10, 40 и 100 Гбит/с). При наличии интеллектуальных инструментов проще и быстрее настроить МСБ под нужды организации. Бесконечное переоснащение тогда не потребуется.

КМСБ реализуют открытую архитектуру и открытые бизнес-процессы, важные для поддержания постоянной гибкости, повышения производительности сети, надежности, гарантированной доставки, безопасности и точности данных. Например, можно фильтровать каналы связи 100, 40 и 10 Гбит/с средствами МСБ, предназначенными для канала 1 Гбит/с; добавить систему обнаружения вторжений и анализатор трафика (сниффер), а также настроить разрешения для пользователей сети — и сделать все эти настройки с помощью одного «клика».

КМСБ устраняет архитектурные ограничения типа SPAN/TAP или избыточные сетевые пути.

Также КМСБ позволяет учитывать изменения и потребности бизнеса организации.

КМСБ продлевает срок службы имеющимся средствам МСБ, например, так, как отмечалось выше, — можно управлять трафиком 10, 40 и 100 Гбит/с средствами МСБ, рассчитанными на 1, 10 и 40 Гбит/с. Масштабируемость сегодня не просто модное слово. Не нужно добавлять все больше и больше новых средств, а нужно только оптимизировать работу имеющихся. Можно купить только требуемое в настоящий момент количество портов и функций, что позволяет более эффективно управлять инвестициями в ИТ.

Или можно использовать имеющиеся сетевые средства с фильтрами — по мере изменения потребностей фильтры настраиваются или добавляются несколькими простыми нажатиями кнопки «мыши». Также при изменении потребностей можно быстро и гибко перераспределить видимость портов любым способом, который больше подойдет в конкретном случае (сверху стойки, в конце ряда или на одном шасси), без изменения расходов на пользовательский интерфейс или управление.

Данные от КМСБ рекомендуется передавать на выделенный для целей МСБ компьютер.

Заключение

Применение КМСБ является достаточно новым, но перспективным направлением обеспечения ИБ от атак со стороны злоумышленников и ненамеренных ошибок персонала в современной сетевой среде организаций. Но данный сегмент рынка еще не столь хорошо представлен, чтобы говорить о его насыщении (хотя уже есть интересные решения типа Director Pro компании Net Optics, Anue Net Tool Optimizer компании Ixia, IntellaPatch Series компании Apcon и другие). В ближайшее время ожидается появление конкурентоспособных продуктов, среди которых организациям необходимо будет сделать осознанный выбор. В статье изложены основы использования КМСБ, полезные при ознакомлении с данной категорией средств ОИБ.

СПИСОК ЛИТЕРАТУРЫ:

1. *Милославская Н. Г., Сенаторов М. Ю., Толстой А. И.* Проверка и оценка деятельности по управлению информационной безопасностью. Учебное пособие для вузов. М.: Горячая линия—Телеком, 2012. — 166 с. (Серия «Вопросы управления информационной безопасностью». Вып. 5).
2. Security & Compliance Monitoring [Электронный ресурс]. URL: http://www.ixiacom.com/solutions/security-and-compliance-monitoring (дата обращения: 02.10.2013).
3. Засецкий А., Шельгов В. Мониторинг сети ЦОД // Журнал сетевых решений/LAN. 2013. № 5. С. 30—36.
4. *Милославская Н. Г., Сенаторов М. Ю., Толстой А. И.* Управление инцидентами информационной безопасности и непрерывностью бизнеса. Учебное пособие для вузов. М.: Горячая линия—Телеком, 2012. — 170 с. (Серия «Вопросы управления информационной безопасностью». Вып. 3).