УДК 004. 891.3

Я.В. Невойт, А.В. Труш

ИНСТРУМЕНТЫ СИСТЕМЫ МОНИТОРИНГА СОБЫТИЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

В данной статье рассмотрены понятия системы мониторинга информационной безопасности и ее компоненты. Рассмотрены основные этапы внедрения любой системы мониторинга событий информационной безопасности и возможность реализации процесса управления инцидентами информационной безопасности.

Ключевые слова: Мониторинг информационной безопасности, средства защиты информации, рабочие станции.

Понятие системы мониторинга информационной безопасности.

Система мониторинга событий информационной безопасности (СМИБ) предназначена для автоматизации процесса сбора и анализа информации о событиях безопасности, поступающих из различных источников. В качестве таких источников могут выступать средства защиты информации, общесистемное и прикладное ПО, телекоммуникационное обеспечение и др. СМИБ включает в себя следующие компоненты:

- программно-техническая часть – реализуется на основе продуктов по мониторингу событий безопасности класса SIEM (Security Informationand Event Management);
- документационная часть - включает в себя набор документов, описывающих основные процессы, связанные с выявлением и реагированием на инциденты безопасности;
- кадровая составляющая - подразумевает выделение сотрудников, ответственных за работу с СМИБ.

Программно-техническая часть СМИБ включаются следующие компоненты:

- агенты мониторинга, предназначенные для сбора информации, поступающей от различных источников событий, включающих в себя средства защиты, общесистемное и прикладное ПО, телекоммуникационное обеспечение и др.;
- сервер событий, обеспечивающий централизованную обработку информации о событиях безопасности, которая поступает от агентов. Обработка осуществляется в соответствии с правилами, которые задаются администратором безопасности;
- хранилище данных, содержащее результаты работы системы, а также данные, полученные от агентов;
- консоль управления системой, позволяющая в реальном масштабе времени просматривать результаты работы системы, а также управлять её параметрами.

На сегодняшний день все больше компаний сталкивается с необходимостью обработки журналов событий, которые регистрируются в информационных системах, с целью выявления возможных атак. При этом даже в небольшой компании в журналах аудита может регистрироваться до нескольких десятков событий в секунду, что делает их анализ в ручном режиме длительным и крайне неэффективным. Для того, чтобы автоматизировать процесс сбора и анализа информации о событиях информационной безопасности могут использоваться специализированные системы мониторинга.

В настоящее время для комплексной защиты от угроз информационной безопасности необходимо использовать различные программные и аппаратные средства. Однако вместе с ростом количества средств защиты существенно увеличивается и объём информации, которую должен обработать администратор безопасности для принятия адекватных решений по реагированию на выявленные атаки. Эффективная работа с большим объёмом данных, поступающих от систем безопасности, требует наличия у администратора высокого уровня квалификации, позволяющего выполнять следующие операции:

- проведение сопоставительного анализа результатов работы различных средств защиты;
- проведение сопоставительного анализа результатов работы средств защиты и параметров работы программно-аппаратного обеспечения системы;
- поиск информации об одном событии в журналах аудита различных средств защиты;

- анализ защищенности сети.

Для автоматизации процесса сбора и анализа информации, поступающей от различных средств защиты предлагается комплексное техническое решение по мониторингу информационной безопасности автоматизированной системы предприятия.

Описание решения.

Реализация функций мониторинга событий информационной безопасности позволит существенно облегчить процесс принятия администратором решения по реагированию на события, связанные с нарушением безопасности и, тем самым, повысить оперативность принятия решении в части реагирования на выявленные инциденты. В состав системы мониторинга включаются следующие компоненты:

- агенты мониторинга, предназначенные для сбора информации, поступающей от различных средств защиты;
- сервер событий, обеспечивающий централизованную обработку информации о событиях безопасности, которая поступает от агентов. Обработка осуществляется в соответствии с правилами, которые задаются администратором безопасности;
- хранилище данных, содержащее результаты работы системы, а также данные, полученные от агентов;
- консоль управления системой, позволяющая в реальном масштабе времени просматривать результаты работы системы, а также управлять её параметрами.

Типовая структура системы мониторинга информационной безопасности отображена на рисунке 1.

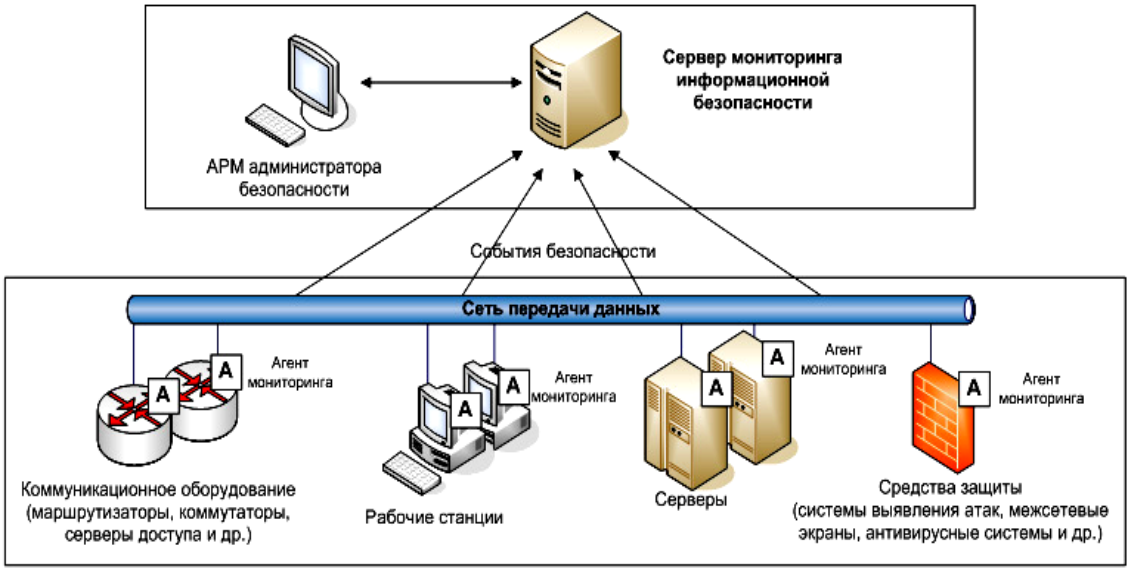

Рис.1. Структура системы мониторинга информационной безопасности

Документационная часть СМИБ предполагает разработку пакета нормативных документов по управлению инцидентами безопасности. Как правило, для этого формируется политика управления инцидентами ИБ, которая определяет классификацию инцидентов, общий порядок реагирования, ответственность за реализацию данного документа и др. На основе данной политики для каждого из видов инцидентов безопасности разрабатывается отдельный регламент, описывающий детальный порядок реагирования на различные виды инцидентов.

Кадровая составляющая СМИБ предполагает выделение различных ролей, ответственных за сопровождение центра.

Как правило, выделяют следующие роли в составе СМИБ:

- системный администратор, отвечающий за поддержку общесистемного аппаратного обеспечения СМИБ;
- администратор безопасности, обеспечивающий управление настройку параметров функционирования СМИБ;
- оператор, выполняющий задачи просмотра результатов работы СМИБ и реализации базовых функций реагирования на типовые инциденты;
- аналитик, обеспечивающий анализ и реагирования на сложные виды инцидентов.

Основные этапы создания СМИБ.

Процесс внедрения любой системы мониторинга событий информационной безопасности включает в себя следующие основные этапы:

1. Обследование автоматизированной системы. В рамках обследования проводится идентификация основных источников событий безопасности, определение технологии сбора, хранения и обработки данных. По результатам обследования формируются требования к архитектуре и функциональным возможностям системы мониторинга информационной безопасности.
2. Разработка технического проекта, в котором описывается конфигурация оборудования и программного обеспечения, порядок внедрения, схема информационных потоков, требования к внешнему окружению системы мониторинга и т.д.;
3. Обучение сотрудников, которые будут отвечать за эксплуатацию системы мониторинга информационной безопасности;
4. Создание пилотного района для тестового внедрения системы мониторинга информационной безопасности. Если объектом мониторинга является территориально-распределённая система, охватывающая несколько филиалов, то в качестве тестового сегмента, как правило, выбирается наиболее крупное подразделение, на котором можно апробировать решения, описанные в техническом проекте.
5. Промышленное внедрение системы мониторинга. Внедрение проводится с учетом результатов, полученных в процессе тестового внедрения системы мониторинга;
6. Техническое сопровождение системы мониторинга информационной безопасности.

Как правило, на этапе создания СМИБ подразделение информационной безопасности старается подключить систему мониторинга к наибольшему количеству источников и получить от них максимальный объем информации. Однако необходимо принимать во внимание тот факт, что если включить все возможные режимы аудита, то это может привести к значительному увеличению нагрузки на серверы, с которых получается информация, и, как следствие, нарушению их работоспособности. Именно поэтому одной из задач на этапе обследования является поиск компромисса между желанием подразделения ИБ получать и обрабатывать максимальный объем информации и реальной возможностью подразделения ИТ предоставить данную информацию.

Еще одной важной задачей, которая должна решаться в процессе внедрения, является определение тех инцидентов, которые будут выявляться в процессе работы СМИБ. Для этого выполняются следующие действия:

- определение типов основных инцидентов ИБ;
- определение списка событий, которые ведут к инциденту ИБ;
- определение источника инцидента ИБ;
- определение и приоритезация рисков, связанных с инцидентами ИБ.

Решение по мониторингу информационной безопасности базируется на продукте *Arc Sight ESM.*

Преимущества решения

- увеличение скорости реагирования на инциденты, связанные с нарушением информационной безопасности;
- автоматизация процесса обработки информации, поступающей от различных средств защиты;
- повышение эффективности управления информационной безопасностью автоматизированной системы.

Возможности HP Arc Sight.

Система мониторинга и корреляции событий HP *Arc Sight* позволяет собирать и анализировать сообщения о событиях безопасности, поступающих от средств защиты, операционных систем, прикладного программного обеспечения и др. Данная информация собирается в едином центре, обрабатывается и подвергается анализу в соответствии с заданными правилами по обработке событий, связанных с информационной безопасностью. Результаты анализа в режиме реального времени предоставляются администраторам безопасности в удобном виде для принятия решений по реагированию на инциденты безопасности.

Технология функционирования *Arc Sight* предусматривает разделение процесса обработки событий безопасности на пять основных этапов: фильтрация, нормализация, агрегирование, корреляция и визуализация. В процессе фильтрации система удаляет события, которые не имеют прямого отношения к инцидентам информационной безопасности. На этапе нормализации события приводятся к единому формату сообщений *Arc Sight.* Агрегирование позволяет удалить повторяющиеся события, описывающие один и тот же инцидент. Эта процедура позволяет значительно сократить объем информации, которая хранится и обрабатывается в системе мониторинга информационной безопасности. Сформированные сообщения затем обрабатываются, используя механизмы корреляции, основанные на статистических методах, а также правилах встроенной экспертной системы. И, наконец, *Arc Sight* выдает полученные результаты на централизованную консоль, работающую в режиме реального времени.

Arc Sight позволяет администраторам безопасности сфокусироваться на реальных угрозах безопасности, обеспечивая их средствами, позволяющими оперативно реагировать на угрозы безопасности сети.

Информационные ресурсы интегрируются в систему мониторинга в качестве источников сообщений о событиях информационной безопасности с помощью так называемых коннекторов (агентов).

Для визуализации результатов работы системы используется консоль администратора, которая в реальном режиме времени позволяет проводить разделение событий по категориям, корреляцию событий, как по ресурсам, так и по злоумышленникам, а также осуществлять подробный анализ. С помощью карты нарушений безопасности можно получить представление об отклонениях в параметрах безопасности. Кроме того, консоль снабжена интуитивно понятным инструментальным интерфейсом и предоставляет непревзойденные возможности для подготовки табличных и графических отчетов о безопасности.

Arc Sight позволяет осуществлять мониторинг информационной безопасности всех необходимых ресурсов в режиме реального времени, получая информацию как на уровне средств защиты, так и на уровне сетевых ресурсов, приложений и баз данных, что позволяет построить комплексную систему мониторинга и управления событиями информационной безопасности.

Еще одной особенностью системы *Arc Sight* является возможность реализации процесса управления инцидентами информационной безопасности строго в соответствии с стандартом PCI DSS.

Заключение.

На сегодняшний день всё больше и больше компаний приходят к пониманию того, что использование СМИБ позволяет значительно повысить эффективность процесса управления инцидентами информационной безопасности. Это обеспечивается за счет автоматизации процесса сбора и анализа информации, которая регистрируется в автоматизированной системе компании. При этом внедрение СМИБ также позволяет значительно повысить эффективность уже установленных в организации средств защиты и получить инструмент для оценки эффективности работы подразделения информационной безопасности.

Література

1. Система функционального активного мониторинга FLAME / В.А. Васенин, В.В. Корнеев, М.Ю. Ландина, В.А. Роганов // Программирование. – 2003. – №3. – С. 161-173.

2. Information technology. Security techniques. Code of practice for information security management: ISO 17799: 2005. – London: The International Standards Glossary, 2005. – 34 p. – (Міжнародний стандарт).

3. Юдін О.К. Захист інформації в мережах передачі даних / О.К. Юдін, О.Г. Корченко, Г.Ф. Конахович. – К.: Вид-во ТОВ „НВП „Інтерсервіс", 2009. – 716 с.

4. Сугоняк І.І. Модель системи підтримки прийняття рішень з оптимального керування життєвим циклом інноваційних проектів підприємств / І.І. Сугоняк // Вісник КДТУ. – Серія: технічні науки. – 2007. – № 43 (4). – С. 91-99.

5. Система функционального активного мониторинга FLAME / В.А. Васенин, В.В. Корнеев, М.Ю. Ландина, В.А. Роганов // Программирование. – 2003. – №3. – С. 161-173.

Надійшла 06.12.2016 р. Рецензент: д.т.н., проф. Чичикало Н.І.