Особенности использования практических инструментов для выявления и расследования инцидентов безопасности

Виктор Сердюк, генеральный директор ЗАО «ДиалогНаука»

На сегодняшний день практически любая компания хотя бы раз сталкивалась с инцидентами в области информационной безопасности (ИБ). Согласно ГОСТ Р ИСО/МЭК 18044 под инцидентом безопасности понимается событие, являющееся следствием одного или нескольких нежелательных или неожиданных событий ИБ, имеющих значительную вероятность компрометации бизнес-операции и создания угрозы ИБ. Инциденты могут являться следствием халатных действий сотрудников или же результатом деятельности киберпреступников. Примерами инцидентов являются: кража конфиденциальной информации, отказ в обслуживании бизнес-приложений, искажение ключевых информационных активов, нарушение требований действующего законодательства и т.д. В рамках данной статьи будут рассмотрены некоторые примеры использования специализированных средств, позволяющих автоматизировать процессы выявления и последующего расследования инцидентов.

Процесс управления инцидентами безопасности

Согласно ГОСТ Р ИСО/МЭК 18044 процесс управления инцидентами ИБ может включать в себя четыре основных этапа (рис. 1):

- Планирование и подготовка (Plan and Prepare) – на данном этапе осуществляется разработка нормативных документов, направленных на формализацию процесса управления инцидентами;
- Использование (Use) – на данном этапе регистрируются события безопасности, а также принимается решение являются ли они инцидентами. Кроме этого здесь также осуществляется реагирование на выявленные инциденты;
- Анализ (Review) – этап, который предполагает определение причин возникновения инцидента и определение мер, которые позволят предотвратить подобные инциденты в будущем;
- Улучшение (Improve) – на последнем этапе реализуются изменения, которые позволят предотвратить появление подобных инцидентов в будущем.

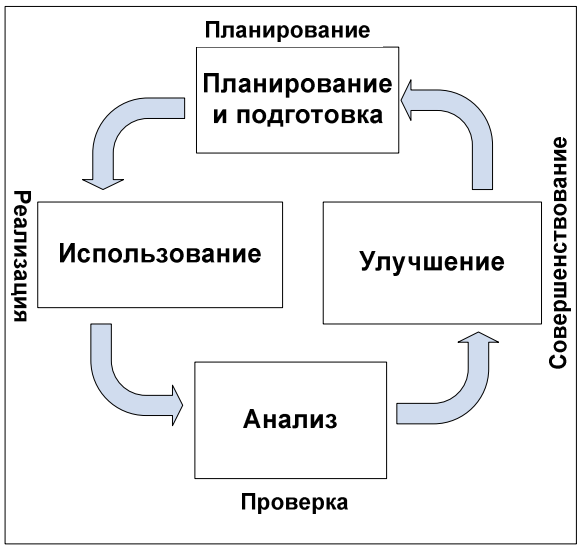

Рис. 1. Процесс управления инцидентами безопасности

Представленная модель управления инцидентами аналогична модели PDCA (Plan-Do-Check-Act), заложенной в основу систем менеджмента информационной безопасности, которая описана в международном стандарте ISO 27001.

Как можно видеть из приведенной выше диаграммы процесс управления инцидентами ИБ должен начинаться с разработки соответствующего пакета документов. Как правило, для этого формируется политика управления инцидентами ИБ, которая определяет классификацию инцидентов, общий порядок реагирования на них, 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.

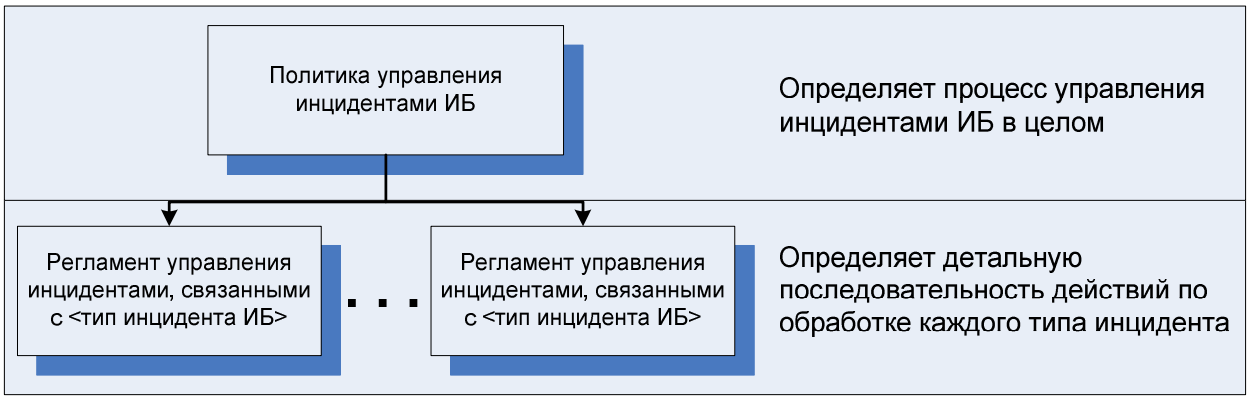

Рис. 2. Структура документационного обеспечения по расследованию инцидентов безопасности

Небольшие и средние компании в большинстве случаев реализуют задачи по выявлению и расследованию инцидентов без использования специализированных средств, позволяющих автоматизировать данные процессы. В этом случае компании разрабатывают необходимые документы, относящиеся к первому этапу цикла управления инцидентами, а процесс выявления и анализа выполняется в ручном режиме.

Для крупных компаний с территориально-распределенными автоматизированными системами эффективное управление инцидентами может быть реализовано только с использованием специализированных средств. Так, для автоматизации процесса выявления инцидентов могут использоваться решения класса SIEM (Security Information and Event Management), а расследование инцидентов может осуществляться более эффективно при условии применения средств класса network forensics. Ниже будут более подробно рассмотрены два этих класса решений.

Автоматизация процесса выявления инцидентов безопасности

Для автоматизации процесса выявления инцидентов, которое осуществляется на этапе «Использование» соответствующего цикла управления (рис. 1), могут применяться системы мониторинга, состоящие из следующих компонентов:

- агенты мониторинга, предназначенные для сбора информации, поступающей от различных источников, включая средства защиты, общесистемное и прикладное ПО, телекоммуникационное оборудование и т.д.;
- сервер событий, обеспечивающий централизованную обработку информации о событиях безопасности, которая поступает от агентов. Обработка осуществляется в соответствии с правилами, которые задаются администратором безопасности. Именно

эти правила позволяют определять инциденты на основе зафиксированных событий 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 рис. 3, приведенном ниже.

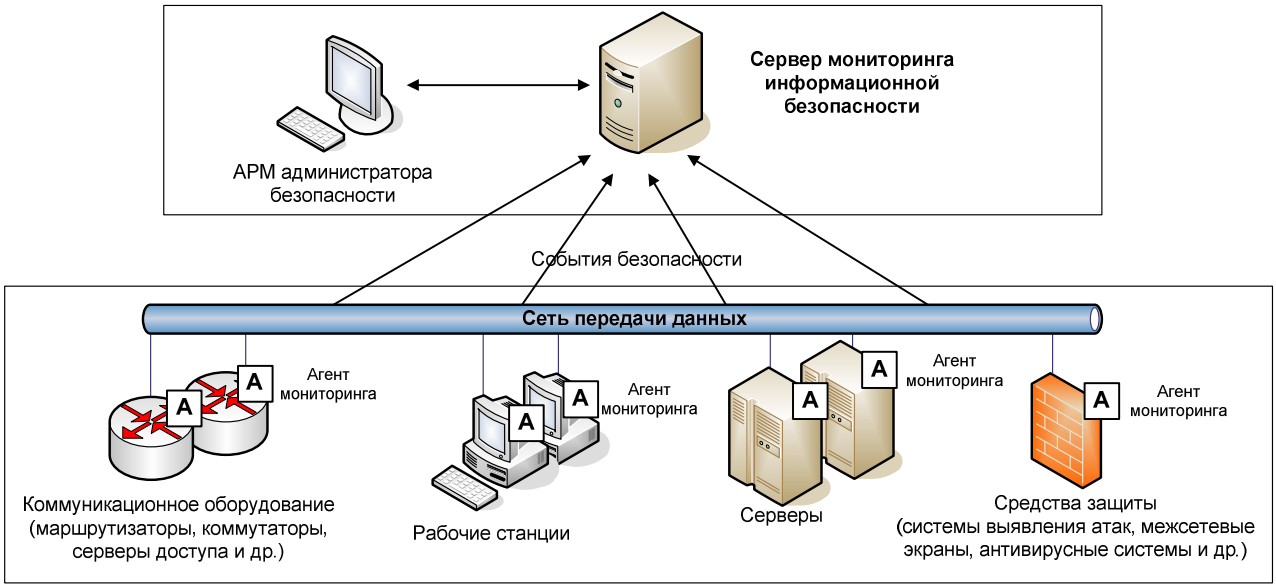

Рис. 3. Структура системы мониторинга информационной безопасности

В настоящее время наибольшее распространение получили следующие коммерческие системы мониторинга событий информационной безопасности: ArcSight, Cisco MARS, RSA Envision, NetForensics, NetIQ, Symantec, и др. Необходимо отметить, что кроме коммерческих существуют также и бесплатные системы мониторинга с открытым кодом. Примером такой системы является продукт Prelude Universal SIM.

Данный класс систем позволяет автоматизировать процесс сбора и анализа информации, поступающей из большого количества источников. Так, система может получать на входе десятки тысяч событий в секунду, а на выходе формировать список из десяти наиболее опасных инцидентов, на которые необходимо реагировать в первую очередь. Обработать такой объем информации в ручном режиме практически невозможно.

Кроме этого, системы мониторинга также позволяют автоматизировать базовые

функции реагирования на выявленные инциденты. Так, например, SIEM-система может проинформировать администратора безопасности о факте возникновения инцидента, а также запустить какое-то внешнее приложения для выполнения определенных задач.

Автоматизация процесса расследования инцидентов безопасности

В ряде случаев после выявления инцидента средствами SIEM-системы возникает задача по его расследованию. Основная цель расследования заключается в сборе доказательной базы, точной идентификации нарушителя и тех методов, которые были использованы для реализации инцидента. Для решения этой задачи часто оказывается недостаточно той информации, которая регистрируется агентами SIEM-системы, а также другими средствами защиты информации. Так, например, в случае выявления инцидента, связанного с утечкой конфиденциальной информации со стороны одного из сотрудников компании, может возникнуть задача по сбору и анализу дополнительной информации о тех действиях, которые совершал сотрудник до и после инцидента. Для решения этих задач могут использоваться решения класса «network forensics», которые позволяют автоматизировать процесс расследования, который относится к этапу «Анализ» цикла управления инцидентами (рис. 1). Примерами таких решения являются средства защиты информации Дозор-Джет, NetWitness Next Gen и др.

Несколько слов хотелось бы уделить решению NetWitness, поскольку оно обладает уникальными свойствами масштабируемости и может быть использовано в компаниях и предприятиях любого масштаба.

Netwitness NextGen реализует задачи по мониторингу сети с помощью трехкомпонентной архитектуры: декодер — концентратор — брокер. Декодер, это базовый компонент всей инфраструктуры Netwitness, который отвечает за сбор и хранение пакетов данных. Декодеры передают собранные данные концентраторам, которые в режиме реального времени объединяют метаданные для анализа и в свою очередь передают их в брокер — устройство, позволяющее в режиме реального времени получить полную картину работы сети для всего предприятия. Все компоненты Netwitness NextGen поставляются в виде программно-аппаратных комплексов (appliance’ов).

Различные варианты платформы позволяют подобрать именно те компоненты продукта, которые соответствуют топологии конкретной сети и отвечают требованиям производительности каждой системы. Анализ трафика в режиме реального времени позволяет отслеживать перемещение информации, контролировать потоки информации и не просто собирать доказательства нарушений, но и предотвращать возможные попытки

передачи конфиденциальной информации.

В отличие от других предложенных на рынке продуктов для перехвата пакетов и мониторинга сети, NetWitness NextGen полностью «собирает» и нормализует сетевой трафик на каждом уровне модели OSI. При этом сбор и анализ информации осуществляется в реальном масштабе времени, чтобы максимально оперативно выявлять и реагировать на инциденты безопасности. Необходимо отметить, что декодеры позволяют собирать и анализировать информацию со скоростью до 1 Гбит/с.

NetWitness NextGen позволяет интегрироваться на уровне интерфейса с системами мониторинга информационной безопасности, например, с ArcSight ESM и RSA Envision. Это позволяет создать на основе этих продуктов полноценный центр управления информационной безопасностью, обеспечивающий не только обнаружение, но и последующее расследование инцидентов безопасности.

Заключение

На сегодняшний день всё больше и больше компаний сталкиваются с необходимостью повышения эффективности процесса обнаружения и расследования инцидентов информационной безопасности. Одним из возможных решений данной проблемы является разработка необходимых нормативных документов, а также использование специализированных средств класса SIEM и network forensics. Практика показывает, что реализация этих мер позволяет значительно снизить ущерб, который наносится компаниям в случае возникновения инцидентов безопасности.