УДК 004.056

Д.С. Муравьева, А.М. Губарь

ОЦЕНКА СООТВЕТСТВИЯ УРОВНЯ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ МИРОВЫМ И ГОСУДАРСТВЕННЫМ СТАНДАРТАМ

Рассмотрены вопросы оценки соответствия уровня безопасности персональных данных, содержащихся в информационных системах, мировым и государственным стандартам. Постоянный мониторинг состояния крупных информационных систем предлагается осуществлять с помощью SIEM-систем. Обсуждаются перспективы такого подхода.

E-mail: triaaaaam@gmail.com, gam46@inbox.ru

Ключевые слова: *персональные данные, законодательство, информационная система, информационная безопасность, системы управления событиями и инцидентами безопасности, SIEM.*

В современном мире информатизация различных сфер человеческой деятельности достигла небывалого размаха и продолжает расширяться все больше. Уже ни одна компания или государственное учреждение не представляют своей работы без информационных систем (ИС), работа которых в свою очередь обеспечивается ИТ-инфраструктурой – компьютерами, серверами, многофункциональными устройствами, объединенными в сети.

Компьютеризация общества коснулась законодательных органов, так как законами и нормативными актами должны регулироваться все сферы жизни общества, поэтому в настоящее время предъявляются определенные требования к ИТ-инфраструктуре и государственных, и коммерческих организаций. Эти требования служат достижению различных целей:

- унификация и стандартизация обработки данных в рамках определенной отрасли;
- обеспечение безопасности конфиденциальной информации;
- защита и реализация прав и законных интересов граждан, чьи данные обрабатываются в конкретных ИС.

Для выполнения последнего пункта наша страна присоединилась к Конвенции Совета Европы «О защите физических лиц при автоматизированной обработке персональных данных», и был разработан Федеральный Закон «О персональных данных» №152-ФЗ [1]. Исходя из определений, сформулированных в указанном законе, любая ИС, в которой обрабатываются какие-либо данные о физическом лице, попадает под действие этого закона и подзаконных актов. Отсюда сле-

дует, что любая компания, которая просто ведет учет сотрудников, должна соблюдать требования данного Федерального закона.

После введения в действие ФЗ-152 и подзаконных документов многие компании и государственные учреждения были вынуждены привести свои ИС в соответствие с ним. И хотя в момент внедрения системы защиты информации она, как правило, соответствует требованиям законодательства, впоследствии, через несколько лет эксплуатации, оценить ее соответствие этим требованиям представляется нетривиальной задачей, решение которой приводит к значительным материальным и особенно временны́м затратам.

В современном мире репутация многих компаний зависит от того, насколько качественно они обеспечивают безопасность персональных данных своих клиентов. Ведь одна утечка базы данных может стоить компании миллионы долларов. При этом компания может выиграть от возможности в любой момент времени подтвердить соответствие своей ИС требованиям законодательства. Поэтому необходимо постоянно отслеживать состояние информационной системы (ИТ-инфраструктуры).

Источниками информации о состоянии ИТ-инфраструктуры являются журналы событий ее элементов. Элементами инфраструктуры могут быть программное обеспечение (ПО), операционные системы (ОС), средства доверенного доступа (электронные замки, средства защиты от несанкционированного доступа), коммутационное оборудование (коммутаторы, маршрутизаторы), межсетевые экраны (программные и аппаратные).

Кроме того, источниками событий могут быть системы контроля и управления доступом, датчики объема, охранные системы и пр.

Для отслеживания состояния информационной системы и системы защиты существует несколько способов:

1) мониторинг состояния ИТ-инфраструктуры вручную. При таком способе мониторинга необходимо просматривать журналы событий требуемого ПО на всех ПЭВМ, сетевых устройствах ИС и средствах защиты информации. Это очень трудоемкий способ, он требует больших временны́х затрат и применяться может только в случае очень небольших ИТ-инфраструктур;

2) мониторинг состояния ИТ-инфраструктуры с помощью средств централизованного управления ПО и средствами защиты. Такой способ мониторинга более результативен и нагляден, требует меньше усилий. Специалист ИТ или информационной безопасности (ИБ) может просматривать журналы необходимого ему ПО на своем рабочем месте (при условиях правильной настройки данного ПО). Однако, учитывая огромное разнообразие различного ПО и средств защиты в современных ИТ-инфраструктурах, специалисту ИТ/ИБ придется просматривать сообщения от многих ис-

точников, при этом бóльшая часть этих сообщений будет нести информацию о рядовых событиях в системе, и среди таких сообщений легко пропустить что-либо действительно важное. А в случае инцидента ИБ расследование займет много времени, так как придется вручную сопоставлять данные от разного ПО, сетевого оборудования и средств защиты;

3) мониторинг состояния ИТ-инфраструктуры с помощью систем управления событиями и инцидентами безопасности (SIEM – Security Information and Event Management). Такие системы позволяют сосредоточить данные со всего ПО, сетевого оборудования и средств защиты на одном экране, выделить самое главное, найти взаимосвязи между событиями и выполнить определенные действия при наступлении того или иного события. Это наиболее подходящий способ мониторинга состояния ИТ-инфраструктуры для компаний, имеющих большую распределенную сеть.

Основными задачами SIEM-систем являются:

- оперативное обнаружение атак и нарушений политики ИБ;
- соотнесение в режиме реального времени событий от разных устройств, выявление инцидентов ИБ и их приоритезация;
- автоматическое реагирование на инциденты;
- формирование базы знаний по инцидентам;
- проведение аудитов и расследований инцидентов;
- оценка уровня угроз для отдельных корпоративных ресурсов [2].

Внедрение системы управления событиями и инцидентами безопасности позволит достигнуть следующих целей:

- обеспечить централизованное управление событиями и инцидентами ИБ путем интеграции существующих в организации сенсоров безопасности и источников данных аудита в единую систему управления;
- увеличить скорость выявления, расследования и реагирования на инциденты безопасности, в том числе обеспечить автоматическое реагирование на инциденты;
- управлять инцидентами ИБ;
- повысить эффективность управления рисками ИБ;
- повысить уровень соответствия политикам и нормативным требованиям, контролировать уровень соответствия системы заданным политикам безопасности (в частности, требованиям законодательства в области персональных данных);
- обеспечить наиболее оперативное устранение сбоев в работе ИТ-инфраструктуры. При этом не важно, чем вызваны сбои – ошибкой пользователя, неисправностью оборудования или атакой на корпоративную сеть [3].

Кроме приведенных выше функций на такую систему можно возложить еще целый ряд задач, решения которых принимаются на основе анализа событий в ИТ-инфраструктуре.

Выполнение всех этих функций SIEM-системой обеспечивается за счет того, что система в автоматическом режиме соотносит данные от различных источников, и используя заданные правила корреляции событий, делает вывод о том, что произошло в системе: например, имел ли место инцидент безопасности или произошел сбой в работе оборудования. Такой подход к анализу событий в ИТ-инфраструктуре позволяет, не отвлекаясь на ложные сигналы тревоги от отдельных средств защиты, анализировать реально опасные ситуации, снижает процент ошибок в обработке событий от элементов ИТ-инфраструктуры, связанный с человеческим фактором.

Для внедрения SIEM-системы в существующую ИТ-инфраструктуру необходимо выполнить ряд подготовительных мер:

- описать круг задач, который должен решаться данной системой в будущем;
- провести оценку решений, присутствующих на рынке;
- определить возможность интеграции используемых систем в компании с выбранным решением;
- выбрать опытного интегратора либо обеспечить работу по внедрению силами специалистов компании-разработчика системы;
- построить топологию сети с учетом внедряемого решения;
- составить список первичных правил корреляции и отчетов;
- определить ответственного за ведение проекта, обеспечить его полномочиями и ресурсами.

Проблема безопасности персональных данных и оценки соответствия ИТ-инфраструктуры определенным требованиям, предъявляемым законодательством и диктуемым современным обществом, остро встает перед компаниями, работающими на современном рынке. При этом каждая компания выбирает способы решения данной проблемы, подходящие именно ей по соотношению затрат и получаемого результата. SIEM-системы могут быть эффективны в качестве инструмента для оценки соответствия ИТ-инфраструктуры законодательству в области персональных данных, но такое решение представляется наиболее удобным и экономически выгодным для достаточно больших организаций, объем обрабатываемых данных в которых не позволяет осуществлять мониторинг событий в ИТ-инфраструктуре вручную. При осуществлении соответствующих настроек для конкретной сети организации такое решение поможет сэкономить на содержании штата ИТ/ИБ специалистов и в каждый момент времени иметь представление о состоянии ИБ в организации.

СПИСОК ЛИТЕРАТУРЫ

1. Законодательство по персональным данным (http: //www. zki. infosec. Ru / law / personal/).
2. Б а ш л ы к о в М.: «Мониторинг, анализ и управление ИБ» (http: //www. itsec. ru/articles2/control/monitoring_analiz_upravl_ib).
3. Актуальность и особенности внедрения решений класса SIEM (http: //www. risspa. ru/node/354).

Статья поступила в редакцию 14.05.2012