АУДИТ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В КОМПЬЮТЕРНОЙ СЕТИ НЕБОЛЬШОГО ПРЕДПРИЯТИЯ

Я.Л. Могилёвчик

Обсуждаются результаты аудита информационной безопасности в компьютерной сети небольшого предприятия. Сеть включает 84 компьютера, 7 принтеров, 3 МФУ и 3 физических сервера. Структура сети представляет собой 2 соединенных 10-портовых коммутаторов D-Link DSG-1210-10P и порядка 9 подключенных к ним и друг к другу различных неуправляемых коммутаторов.

В ходе аудита были определены области правильного функционирования сети, исследованы уязвимости и риски, обследованы возможности защиты периметра, защиты сегментов сети, содержащих общедоступные сервисы и отделяющие их от частных (демилитаризованых зон сети) и другие работы. Особое внимание было уделено инспекции пакетов с хранением состояния (Stateful Packet Inspection), что позволило дополнительно защититься от атак, выполняя проверку проходящего трафика на корректность.

В докладе показано, что проведенный аудит дал возможность полностью окупить затраты на свое проведение (как материальных, так и человеческих ресурсов) за счет сокращения инцидентов информационной безопасности в сети по окончании аудита (сократились затраты на ликвидацию инцидентов).

О ФОРМИРОВАНИИ ЦЕНТРАЛИЗОВАННОГО АУДИТА СОБЫТИЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В СОСТАВЕ ПОДСИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИОННЫХ СИСТЕМ РЕСПУБЛИКИ БЕЛАРУСЬ

А.О. Молчан, О.Э. Сязанцев

В силу быстро растущей информатизации общества количество хранимой, обрабатываемой и передаваемой в электронном виде информации растет в геометрической прогрессии. Возникает острая необходимость в контроле и ограничении доступа к обрабатываемой информации, а также в своевременной информированности ответственных за информационную безопасность (далее – ИБ) лиц об инцидентах ИБ. Помимо общедоступности информации уязвимость информационных систем (ИС) возрастает также за счет повышения сложности элементов ИС, появления новых технологий передачи и хранения данных, увеличения объема программного обеспечения (ПО). Для мониторинга ИС на предмет корректного функционирования всех ее процессов, активов и ресурсов, а также сохранности информации, доступ к которой ограничен, в составе системы защиты информации (СЗИ) ИС организуется подсистема аудита событий ИБ.

Системы аудита событий ИБ используются для мониторинга ИС на предмет корректного функционирования и сохранности информации, доступ к которой ограничен. На данный момент существует множество средств аудита событий ИБ, как встроенных в общесистемное ПО, так и специально разработанных программных и программно-аппаратные комплексов. Однако, в государственных ИС согласно законодательству Республики Беларусь в области защиты информации (ЗИ) допустимо использование только тех средств ЗИ, которые прошли сертификацию по требованиям безопасности информации и получили сертификат соответствия либо экспертное заключение на соответствие требованиям технических нормативных правовых актов в области технического нормирования и стандартизации.

Многие средства ЗИ ведут журналы аудита автономно, и интеграция их производится вручную ответственными за ИБ лицами. Главная проблема формирования централизованного аудита ИБ в составе СЗИ ИС на данный момент является дороговизна иностранных продуктов (в частности, систем SIEM) и ограниченное представление систем аудита ИБ белорусского производства на рынке средств ЗИ, которые также позволяли бы снизить угрозы ИБ.

Для решения данного вопроса были выявлены требования к подсистеме аудита ИБ на основании законодательной базы Республики Беларусь, обеспечивающие максимальную безопасность в современных условиях, проведен анализ средств аудита ИБ представленных в реестре средств ЗИ, утвержденном Оперативно-аналитическим центром при Президенте Республики Беларусь, сформулированы рекомендации по формированию централизованного аудита ИБ.