УДК 004.056

РАЗРАБОТКА ТЕСТОВ ДЛЯ АВТОМАТИЗИРОВАННОЙ ПРОВЕРКИ РАБОТЫ DLP-СИСТЕМЫ ФИНАНСОВОЙ ОРГАНИЗАЦИИ

Волобуева А.А. (Университет ИТМО)
Научный руководитель – кандидат технических наук, доцент Бибиков С.В.
(Университет ИТМО)

Аннотация. В работе проводится исследование возможностей автоматизации проверок корректности работы политик DLP-системы, выбор системы для этих целей. Разработаны тесты, позволяющие проводить данную оценку.

Введение. Законодательство обязывает финансовые учреждения сохранять конфиденциальность сведений о клиентах. DLP-система помогает контролировать и предотвращать возможные утечки конфиденциальной информации. Поэтому важно регулярно проводить тестирование корректности её работы. Ручное тестирование может занимать много времени, в связи с чем не представляется возможным проводить его достаточно часто.

Основная часть. Ручное тестирование системы занимает много времени, так как нужно проверять все возможные каналы утечки. Для автоматизации тестирования в работе предлагается использовать систему класса BAS. Breach & Attack Simulation (BAS, симуляция атак и взломов) – это инструменты, которые позволяют воссоздать полный цикл атаки (включая внутренние угрозы и кражу данных) на корпоративную инфраструктуру с использованием программных агентов, виртуальных машин и других средств. Оценка переданной в результате проводимого тестирования конфиденциальной информации позволит определить корректность внедренных политик DLP-системы. Финансовые организации обязаны сохранять конфиденциальность следующих сведений:

- личные данные клиента (паспортные данные, СНИЛС, ИНН);
- реквизиты юридических лиц;
- сведения об имуществе, находящегося в собственности клиента;
- сведения об уровне доходов;
- данные банковского счета (номер, дата открытия, валюта, информация об остатке по счету, начисляемых процентах);
- данные о кредитах (наличие кредитов, условия кредитования);
- информация о движении денежных средств на счетах.

На основании этого были разработаны тесты, которые содержат образцы данных в различных комбинациях. Файлы для тестирования работы DLP-системы содержат, например, PAN карт (согласно международному стандарту PCI DSS PAN карт не может передаваться в открытом виде, а должен быть маскирован), выписки по счетам, заключения по кредитным заявкам, персональные данные и т.п.

Выводы. В результате были разработаны тестовые файлы для оценки корректности работы настроенных политик DLP-системы. Данные файлы могут быть использованы как для ручной проверки, так и для загрузки в систему BAS. Автоматическое регулярное тестирование работы DLP-системы позволит оперативно узнать о возможных неполадках в её работе.

Волобуева А.А. (автор) Подпись

Бибиков С.В. (научный руководитель) Подпись