Методы тестирования для аудита систем управления информационной безопасностью

УДК 004.056

Виталий Хох[1], Елизавета Мелешко[2]

Центральноукраинский национальный технический университет,
[1]vd.khokh@gmail.com, [2]elismeleshko@gmail.com

На сегодняшний день средний и крупный бизнес все чаще разворачивают личные инфраструктуры, необходимые непосредственно для осуществления предпринимательской деятельности. Вместе с увеличением возможностей для развертывания личных информационных систем: увеличением доступности их компонентов и повышением общей образованности в области информационных технологий – растет и количество «чувствительной» информации, циркулирующей Интернетом или интранетом определенных компаний. Чувствительная информация – информация, несанкционированное раскрытие, модификация или сокрытие которой может привести к финансовому убытку или иному ущербу.

Цель данной работы – исследование методов тестирования систем управления информационной безопасностью, с более широким рассмотрением тестов на проникновение.

Методы тестирования, применяемые в аудите систем управления информационной безопасностью, заключаются в выполнении одного или нескольких оценочных задач при определенных условиях для сравнения ожидаемого (заявленного) поведения оцениваемой сущности с реальной. Если рассматривать метод тестирования в разрезе руководства по аудиту, которое было разработано силами форума специалистов по внедрению серии стандартов ISO27k Forum, то он применяется только в третьей фазе проведения аудита – работе на месте. В руководстве, метод тестирования связывают с чисто техническим процессом, благодаря которому определяется правильность конфигурации информационных систем относительно политики информационной безопасности, стандартов и технических руководств. Также, указывается на возможность использования автоматизированных средств проверки и выявления уязвимостей системы и конфигураций, но предупреждается о том, что, несмотря на повышение скорости этого процесса, есть большая вероятность того, что в отчетах автоматизированных средств будет и искаженная информация, что обусловлено ошибками в самих средствах.

В специальной публикации национального института стандартов и технологий США – NIST Special Publication 800-115, тестирование систем управления информационной безопасностью разделяют на три группы: 1) просмотр методов (техник); 2) идентификация и анализ техник; 3) валидация уязвимостей.

Стоит остановиться на последней группе, которая предполагает тесты на проникновение. Главной задачей тестов на проникновение является определение уязвимостей в контролируемых условиях для того, чтобы от них можно было избавиться до того, как ими воспользуются злоумышленники.

Специалисты используют тест на проникновение для решения проблем, связанных с оценкой рисков, сосредотачиваясь на опасных уязвимостях. Метод тестирования на проникновение предусматривает не только технические средства, например, во время теста может быть предпринята попытка физически добраться к носителям данных или похитить их. Тестирование на проникновение позволяет собрать необходимые для аудита свидетельства соответствия или несоответствия требованиям. Существуют три стратегии проведения теста на проникновение:

• Черный ящик. Стратегия реализуется в случае, когда у специалиста нет никакой информации о цели. В таком случае он собирает информацию с чистого листа, и проводятся все действия и процедуры, которые проводил бы реальный злоумышленник.

• Серый ящик. Специалист имеет определенную информацию о цели, но недостаточную, что заставляет его искать дальше.

• Белый ящик. Реализуется, когда специалисту предоставляют всю необходимую информацию о цели.

Тест на проникновение состоит из трех фаз: подготовка, тест, анализ. При подготовке определяются цели и стратегии; во второй фазе выполняется сбор информации о целях, поиск и анализ уязвимостей, попытки использовать уязвимости; в случае, если уязвимость использована удачно, тест переходит в фазу анализа полученных данных.

Кроме этого к группе тестирования на проникновение относится социальная инженерия, она предусматривает использование социальных навыков для получения паролей, данных о кредитных картах или компромата. Методы социальной инженерии используют внутреннюю природу людей, чтобы манипулировать ими и получать конфиденциальную информацию. Существует пять моделей убеждения в социальной инженерии, основанных на: простоте, любопытстве, разногласиях, уверенности в себе и сопереживании.

Методы тестирования позволяют эффективно проверить адекватность системы, ее способность работать как в рамках штатного режима, так и в режиме атак. Методы тестирования позволяют определить пробелы в системе управления информационной безопасностью, о которых не было сказано в документации, а персонал о них мог и не догадываться.

Рассмотренные методы тестирования требуют высококвалифицированных и высокооплачиваемых специалистов. Автоматизация методов тестирования, применяемых для аудита систем управления информационной безопасностью, позволит усовершенствовать процесс аудита и снизить его стоимость.