Задачи теста на проникновение

Согласно пункту 11.3 требований стандарта PCI DSS, в компании минимум раз в год, а также в случае существенных изменений структуры сети (например, внедрении новых серверов), должен проводиться тест на проникновение. Под тестом на проникновение понимается проведение атак на сетевом уровне и на уровне приложений на все публично доступные сервисы компании из сети Интернет (т.н. "внешний тест на проникновение") и внутренние ресурсы, входящие в область аудита PCI DSS (т.е. внутренний активный аудит защищенности). Тест на проникновение позволяет оценить реальный уровень защищенности информационных ресурсов компании как с точки зрения внешнего злоумышленника, так и с позиции злонамеренного сотрудника компании (инсайдера).

В документе "Information Supplement: Requirement 11.3 Penetration Testing", выпущенном PCI SSC для разъяснения требований пункта 11.3 стандарта PCI DSS, отдельно подчеркивается различие между тестом на проникновение и сканированием сети с использованием сканеров уязвимостей. Сканирование не является достаточной мерой и его проведение не может являться выполнением требований пункта 11.3 стандарта.

Внешний тест на проникновение из сети Интернет

В рамках внешнего теста на проникновение аудиторы проводят полный анализ всех деталей исследуемого объекта, выбирают подходящие сценарии атак с учетом человеческого фактора, возможно, разрабатывают уникальное для каждого конкретного случая программное обеспечение для попытки проникновения в информационную систему. Инструментальные средства (сканеры) используются лишь на этапе подготовки к проведению теста на проникновение, так как инструментальные средства помогают только в тривиальных случаях, когда уязвимости очевидны. Помимо технологических проверок в процессе внешнего теста на проникновение проводится тестирование возможности проникновения в информационную систему с использованием методик социальной инженерии путем почтовой рассылки на адреса электронной почты пользователей специализированно сформированного сообщения.

Рассылка осуществляется по заранее согласованному с Заказчиком фиксированному списку адресов электронной почты сотрудников и в заранее оговоренное время. Функциональные возможности программы строго ограничены алгоритмом, безопасным для информационной системы Заказчика.

Внутренний активный аудит защищенности из корпоративной сети

Согласно используемой методике технологического аудита, в процессе выполнения внутреннего теста на проникновение (активного аудита защищенности) аудиторами выполняется поиск и реализация обнаруженных уязвимостей на каждом сервере, рабочей станции и сетевом оборудовании, входящим в область теста, что позволяет получить реальную картину защищенности информационной системы. Все проводимые технические проверки заранее оговариваются со службами информационной безопасности и информационных технологий. Все проверки изначально разработаны с учетом необходимости обеспечения безопасности и постоянной работоспособности информационной системы Заказчика в процессе проведения работ по аудиту.
При проверках особо критичных ресурсов заранее оговаривается график проведения проверок (вплоть до выполнения определенных проверок в нерабочее время) и постоянный мониторинг критичных ресурсов службой ИТ в процессе проведения проверок для исключения возможности отказа в обслуживании.
Согласно рекомендациям PCI SSC, тестирование может проводиться как с использованием методики "черного ящика" (когда аудитор не обладает никакой информацией о тестируемой сети), так и с использованием методики "белого ящика" (когда аудитору предоставляется схема сети и ряд документов, таких как отчет о предыдущих тестах на проникновение, но не предоставляется никаких логических прав в системе).

Что вы получаете в результате тестирования на проникновение

Отчет, предоставляемый Заказчику по результатам проведения тестирования на проникновение, содержит детальное описание проведенных работ, все выявленные уязвимости системы и способы их реализации. Помимо выполнения требований пункта 11.3 стандарта PCI DSS Заказчик получает комплексную оценку уровня информационной безопасности и разработанные на основе полученных результатов рекомендации по повышению текущего уровня защищенности информационной системы.