УДК 004 **Технические науки**

Дьяченко Никита Владимирович, *студент 3 курса по направлению «Информармационная безопансость», Донской государственный технический университет Россия, г. Ростов-на-Дону*

ТЕСТИРОВАНИЕ ПРИКЛАДНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Аннотация: В данной работе рассматриваются вопросы, касающиеся тестирования прикладного программного обеспечения, систему проверки закупленного оборудования, сертификация и аккредитация.

Ключевые слова: информационная безопасность, сертификация, аккредитация, тестирование оборудования.

Annotation: This paper discusses issues related to testing of application software, verification system of purchased equipment, certification and accreditation.

Keywords: information security, certification, accreditation, equipment testing.

Тестирование прикладного программного обеспечения.

Специалисты по безопасности часто помогают тестировать новые системы или модернизировать существующие. Эти тесты должны быть достаточно тщательными, чтобы убедиться, что проверяется все ожидаемые и неожиданные действия и правильно обрабатываются ошибки. Также должны выполниться тесты для проверки максимальной нагрузки на систему, включая объем транзакций, распределение памяти, ширину полосы пропускания сети и время отклика. Если используете производственные или конфиденциальные данные в тестировании, стоит убедиться, что предпринимаются шаги для обеспечения безопасности этих данных.

Поскольку атаки проверки входных данных очень распространены, сотрудники службы безопасности должны работать с персоналом по

тестированию программного обеспечения, чтобы убедиться, что тесты обнаруживают любые входные уязвимости. Один из видов тестирования входных уязвимостей называется Fuzzing (фаззингом). Fuzzing-это практика предоставления случайного ввода в программное обеспечение, чтобы увидеть, как оно обрабатывает неожиданные данные. Фуззинг может помочь идентифицировать входные вероятности лучше, чем тестеры, пытающиеся думать о плохих входных данных [1].

Системы закупок.

Одним из распространенных способов проникновения новых уязвимостей в окружающую среду является изменение, которое вызывает непреднамеренные побочные эффекты. Нужно тщательно оценить любое изменение в среде, чтобы убедиться, что оно не приведет к появлению новых уязвимостей. Сделайте это с помощью нового оборудования и программного обеспечения. Приобретение нового оборудования является важной ролью специалиста по безопасности, но это может снизить общую безопасность, если процесс не будет обработан должным образом. Каждый раз, когда нужно приобрести новое оборудование, нужно тщательно оценить, какие продукты будут соответствовать требованиям. Чтобы убедиться, что новое оборудование не подвергает среду каким-либо новым уязвимостям, необходимо выполнить следующие действия:

- Оцените различные доступные решения.

- Оцените поставщиков с точки зрения технического обслуживания, поддержки и обучения.

- Используйте общие критерии, чтобы упростить процесс оценки.

- Мониторинг контрактов поставщиков и соглашений об уровне обслуживания (SLA).

- Правильно установить оборудование и формально принять его в конце проекта.

- Соблюдайте процедуры закупок организации, чтобы обеспечить справедливый процесс закупок.

- Мониторинг систем и оборудования для выявления оборудования, срок

службы которого подходит к концу, чтобы запланировать его замену [2].

Общий критерий.

Поскольку приобретение нового оборудования может привести к уязвимостям в системе безопасности, имеет смысл ускорить этот процесс. Необходимость в формальном подходе к оценке систем и оборудования породила несколько различных наборов стандартов. Так, например, правительство США создало серию документов по стандартам компьютерной безопасности, известных как серия Rainbow из-за смелых цветов на обложках документов. В Красной книге описаны компоненты доверенной сетевой инфраструктуры (ТНИ). Оранжевая книга рассказывает о сохранении контроля доступа и конфиденциальности в секретной системе. Оба использовали ряд оценочных уровней (C2, B3 и т. д.), и продавцы оценивали свои продукты на этих уровнях. Разработчики серии Rainbow впервые назвали ее TCSEC.

Другие правительства создали свои собственные эквиваленты. Некоторые начинали с TCSEC и вносили изменения. В конце концов, они слились в то, что стало ITSEC. Правительства Соединенных Штатов, Соединенного Королевства, Канады, Германии, Франции и Нидерландов использовали ITSEC в качестве отправной точки. Затем они разработали новый стандарт закупок под названием "общие критерии" [3].

Общие критерии имеют ряд все более сложных уровней обеспечения оценки (EALs), пронумерованных от 1 (самый низкий) до 7 (самый высокий). Оценочные лаборатории разбросаны по всему миру. Ведущие поставщики внутри отрасли (например, поставщики брандмауэров) коллективно создают стандартное, идеальное и совершенное решение. Любой поставщик может провести оценку своего продукта в соответствии со стандартом. Оценка EAL гарантирует, что требования поставщика соответствуют коллективному стандарту до определенного уровня тестирования. Документация, разработка и производительность продукта должны соответствовать требованиям оценки.

Политика в отношении данных.

Все данные в какой-то момент теряют свою полезность. Лучше всего

просто следовать инструкциям в политике обработки данных. Политики, охватывающие управление данными, должны охватывать переходы на протяжении всего жизненного цикла данных. Надежная политика данных должна содержать разделы или даже полные документы, которые охватывают хранение, а также утилизацию.

В разделах политики хранения и хранения данных должно быть указано, как долго вы будете хранить различные типы данных. Некоторые элементы данных имеют более длительный срок полезного использования, чем другие. Если необходимо хранить исторические данные для исследовательских целей, политика должна касаться того, как их хранить. Политика безопасности должна распространяться и на хранимые данные.

Когда вам больше не нужны данные. можно либо перезаписать данные на носители, чтобы подготовить их к повторному использованию, что называется стиранием, либо уничтожить носитель. Выбор зависит от полезности носителя и чувствительности данных. Для чрезвычайно конфиденциальных данных безопаснее стереть данные и уничтожить носитель, чтобы он не попал в руки того, кто может восстановить все или часть стертых данных.

Всякий раз, когда нужно избавиться от оборудования, стоит убедиться, что избавляетесь от него безопасным способом, чтобы не раскрывать никаких конфиденциальных данных. Доступно несколько вариантов:

- Размагничивание-применение сильной магнитной силы к магнитным носителям обычно делает всю электронику непригодной для использования.

- Физическое уничтожение-физическое уничтожение носителей, на которых хранятся данные, гарантирует, что вы уничтожите любые конфиденциальные материалы.

- Перезапись данных—эта опция не уничтожает носитель вообще. Многократная перезапись данных на носителях повышает вероятность того, что какие-либо данные могут быть восстановлены. Однако по-прежнему сохраняется вероятность того, что решительный человек сможет восстановить некоторые удаленные данные.

Сертификация и аккредитация.

В промежутке между закупкой и утилизацией необходимо убедиться, что компоненты в вычислительной среде соответствуют требованиям. Сертификация — это процесс проверки системы на протяжении всего ее жизненного цикла, чтобы убедиться, что она соответствует заданным требованиям. Аккредитация — это официальное согласие уполномоченного должностного лица принять на себя риск внедрения системы. Процесс включает в себя следующих специалистов:

- Уполномоченное должностное лицо-старший менеджер, который должен рассмотреть отчет о сертификации и принять решение об утверждении системы для внедрения. Уполномоченное должностное лицо официально признает и принимает риск, который система может представлять для агентства, активов или отдельных лиц.

- Сертифицирующий-физическое лицо или команда, ответственная за выполнение теста и оценки безопасности для системы. Сертифицирующий орган также готовит отчет об операционном риске системы.

- Владелец системы-лицо, ответственное за повседневную работу системы и обеспечивающее, чтобы система продолжала функционировать в соответствии с установленными условиями [4].

Библиографический список:

1. Советов Б.Я., Информационные технологии Высшая школа, 2009г.
2. Мельников В.П. Информационная безопасность и защита информации. 3-е изд. Академия. 2008 г.
3. Грушо А.А., Применко Э.А., Тимонина Е.Е. Анализ и синтез криптоалгоритмов. Курс лекций. 2000 г.
4. Варлатая, С.К., Аппаратно-программные средства и методы защиты информации. 2007 г.