Границы применимости организационных мер при эксплуатации СКЗИ или где начинается работа хакеров

Николай Смирнов

smirnovnv@infotecs.ru

конференция
РусКрипто'2013

http://www.ruscrypto.ru/conference/

План доклада

Границы применимости организационных мер при эксплуатации СКЗИ или где начинается работа хакеров

Предпосылки
Причины выбора тематики
Терминология

Проблематика
Информационная небезопасность
Невыполнимые регламенты
Риски и целесообразности

Вопросы
Открытые вопросы
Путь Инфотекс

Форма доклада

infotecs®

Человек с человеком испокон веку ведут монолог.

Станислав Ежи Лец

- В докладе формулируется несколько вопросов
- Предлагаю ответы, при их наличии, высказывать сразу

Предпосылки

События

- Реальные атаки и трансформация восприятия среды функционирования СКЗИ
- Указ 31с и «реальная защищённость»
- Исследования «энтузиастов ИБ» и интерпретация результатов экспертами

Предпосылки

Терминология

- Качество – это соответствие требованиям
- Требования ИБ – модель нарушителя и угроз
- Квалифицированный* аудит – анализ выполнения требований – критерий качества
- Защищенность – системное и комплексное понятие

*Квалифицированный - «Правила игры» известны участникам – сертификация, аттестация и инструментальные исследования

Идеальный комплекс мер

- Объект информатизации исследован и описан
- Зафиксированы информационные потоки бизнес процессов
- Построены планы управления рисками
- Разработана модель нарушителя
- Выбраны и внедрены технические средства
- Сформулированы и внедрены автоматизированные политики безопасности
- Проведено обучение
- Выполнен аудит

СКЗИ и средства ЭП необходимое и/или достаточное?

- Информационная защищенность любого объекта – результат выполнения комплекса мер
- Цель создания СКЗИ или средства ЭП – выполнение целевых функций
- Требования к СКЗИ и средствам ЭП – требования регулятора
- Организационные меры и комплексные методы – неотделимый элемент СКЗИ и средств ЭП

Организационные меры с точки зрения вендора

- Уточнение границ среды функционирования СКЗИ и средств ЭП
- Ориентация на обобщенную модель нарушителя
- Упрощение, ускорение и удешевление работ по созданию целевых функций
- Фокусировка компетенций в границах целевых функций
- Создание сбалансированных линеек продуктов, комбинирующих и комплексирующих целевые функции компонент
- Оптимизация сертификационных активностей

infotecs®

Неработающие организационные меры

- Неопределенная среда функционирования
- Нарушители произвольных типов
- Компромиссы -> Уязвимости

infotecs®

Причины неработающих организационных мер и правил использования

- Отсутствие адекватной оценки рисков ИБ потребителем
- Эргономика средств ИБ
- Минимизация затрат на ИБ
  - Организационные меры – это универсальный джокер выбора методов выполнения требований ИБ
- Вопросы веры
- Неработающие регламенты
  - Чтобы понять, что такое рекурсия, надо сначала понять что такое рекурсия

infotecs®

Примеры

- Делегирование средств квалифицированной ЭП
- Кэширование идентификационной информации (пинкода средств квалифицированной ЭП)
- Сетевой экран с правилом «пропускать все»
- АПМДЗ в шкафу, а не в рабочей станции
- Пароль «qwerty» на post-it
- Отсутствие контроля доступа
- Использование произвольных мобильных устройств
- И т.д. и т.п.

infotecs®

Неприятная реальность

- Нарушитель с правами администратора (администратора домена) и возможностью установки средств отладки, как с физическим доступом, так и удаленно, не предусмотренный в модели и использованных технических средствах

Утопия

Простое понятное невыполнимое решение

Доверенный целостный доверено управляемый аппаратный гипервизор, созданный на доверенном производстве

Где правильная точка?

Качество, репутация и стоимость.

В какой момент целесообразность приводит к уязвимости?

Простые соображения

Парадоксальный критерий

Внедрение технических средств защиты информации не должно ухудшать безопасность защищаемой системы

Где правильная точка?

infotecs®

Качество, репутация и стоимость.

- Качество и глубина проверки на НДВ
  - Статический анализ
  - Code review
  - Аудит всех сценариев использования
- Контроль уязвимостей
  - средств разработки,
  - сред функционирования,
  - используемых сторонних библиотек
- Оптимизация таймаутов в рамках реактивной модели

Вопросы

Открытые вопросы

- Можно ли для СКЗИ и средств ЭП предполагать защиту от НСД на уровне организационных мероприятий? С учетом риска появления внутреннего нарушителя с правами суперпользователя?
- Можно ли делегировать функционал защиты целевых функций технических средств другим техническим средствам? А с учетом их потенциального неиспользования?
- Где граница рентабельности и критериев качества и защищенности?

Путь Инфотекс

Еще не ответ, но попытка

- Аудит уязвимостей продуктов силами дочерней компании «Перспективный мониторинг»
- Безусловное устранение выявленных уязвимостей и НДВ
- Создание собственной испытательной лаборатории
- Постоянные инвестиции в повышение качества производственных процессов
- Переход от ориентации на Администраторов ViPNet на ориентацию на простых пользователей как целевых потребителей
- Расширение продуктовых линеек продуктом IDS
- Развитие системы мониторинга в сторону SIEM next gen

Путь Инфотекс

Ожидания

Постоянное повышение вероятности реальной защищенности

Спасибо за внимание. Давайте поговорим?

Николай Смирнов
Начальник отдела научных исследований и развития продуктов
ОАО «Инфотекс»

smirnovnv@infotecs.ru