infotecs

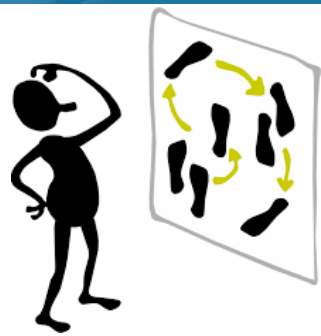
Между регуляторами и потребителями – жизнь в пограничном слое. Практический опыт разработчика средств ИБ.

Дмитрий Гусев
Зам. генерального директора ОАО «ИнфоТеКС»
gusev@infotecs.ru

О компании

- Нам 24 года
- Мы лицензиаты ФСБ России, ФСТЭК России, Министерства обороны
- Мы делаем продукты **ViPNet**:
  - Межсетевые экраны
  - Средства криптографической защиты информации (сетевые, локальные, мобильные)
  - PKI
  - Средства обнаружения вторжений
  - Средства сдачи отчетности в электронном виде
- Вместе с партнерами оказываем услуги проектирования ИС в защищенном исполнении
- Наш опыт – реализовано более сотни тысяч серверных продуктов и порядка миллиона лицензий на клиентские продукты
- Наши заказчики – весь спектр государственных структур, ряд крупных компаний и госкорпораций (РЖД, Роснефть, Росатом, Ростелеком)

О требованиях регуляторов…



- Требования ФСБ России к СКЗИ, СОА, УЦ
- Требования ФСТЭК России к СЗИ от НСД, СОВ, методология Общих критериев
- Требования и стандарты отраслевых регуляторов (Минкомсвязь, Банк России, Газпром, МО и т.д.)
- Международные стандарты и рекомендации (ISO, PCI DSS, FIPS и т.д.)

… и проблемах, с ними связанных

- Требований много, продукт один (например, межсетевой экран)
- Часть требований носит закрытый характер (ФСБ России) и не покрыта методическими рекомендациями
- Требования разных регуляторов построены по разным методологиям
- Многие требования дублируют друг друга – это хорошо… но, проверка на соответствие этим требованиям проводится разными лабораториями и не согласованно (например, проверка по требованиям отсутствия НДВ)
- Изменения в требования вносятся очень долго и отстают от реалий рынка

О требованиях заказчиков...

- Бизнес-требования первичны, под них выбираются соответствующие ИТ - ИБ по факту обсуждается в последнюю очередь
- Требования к СЗИ формируются с учетом характеристик лучших мировых образцов, даже если эти образцы не доступны на локальном рынке или заказчик не может себе позволить их приобрести
- Хочу мобильных сервисов
- Пришествие сервисной модели или меняем CAPEX на OPEX

... и проблемах, с ними связанных

- Часто требования не соотносятся с реальными задачами
- Требования регуляторов преимущественно воспринимаются в лучшем случае как «налог на ИТ», в худшем – «вы засланцы наших спецслужб»
- Постоянное желание сэкономить на ИБ – в первую очередь на проектных работах
- Отсутствие модели нарушителя и угроз, соответствующей реальной ситуации

Неблагоприятные факторы

- Санкции пришли: ограничения на поставки ряда электронных компонент, снижение маржинальности – все это на фоне практически отсутствующей электронной промышленности в России
- Увеличение количества и качества киберугроз
- Apple, Microsoft, Google – курс на изоляцию операционных систем «больше сервисов конечному потребителю, все в «облака», мы печемся о вашей безопасности»
- Усиливающийся дефицит профессиональных кадров – все чаще у молодых специалистов обнаруживается эффект «клипового мышления»

Или импортозамещение нам поможет?

Практический опыт ИнфоТеКС

- Внедрение практик безопасной разработки кода (SDL), публикация политики ответственного разглашения и организация процесса реагирования на выявленные уязвимости в продуктах
- Создание выделенного подразделения со специалистами и экспертами в области практической безопасности – ЗАО «Перспективный мониторинг»
- Создание выделенного подразделения с функциями исследовательской лаборатории и получение аттестата аккредитации ФСБ России
- Создание лаборатории нагрузочного тестирования продуктов
- Ведутся работы по созданию центра мониторинга сетевых атак (в т.ч. в рамках развития темы ГосСОПКА)
- Взаимодействие с ФСБ России по согласованию он-лайн схемы распространения СКЗИ
- Технологическое партнерство с отечественными и зарубежными поставщиками аппаратного обеспечения, в т.ч. разработчиками мобильных платформ (YotaDevices, Samsung, Motorola)
- Участие в нормотворческой деятельности и разработке рекомендаций в рамках ТК26 и ТК362, в т.ч. международной деятельности по стандартизации российских криптоалгоритмов

Ожидаемые результаты

- Повышение уровня доверия коммерческих заказчиков к продуктам ViPNet и компании в целом
- Улучшение функциональных качеств продуктов ViPNet за рамками обязательных требований регуляторов
- Соответствие параметров СЗИ ViPNet современному уровню киберугроз и переход к инцидентной модели реагирования на выявленные проблемы (уязвимости ИС, уязвимости СЗИ, ошибки, реализация доработок функциональности)

infotecs

Спасибо за внимание!