БАНК SIAB
Практичные решения для жизни

7 лет поиска.

Что, как и зачем мы проверяем.

НИКИТИН А.В

19.02.2015

УРАЛЬСКИЙ ФОРУМ

7 ЛЕТ. История вопроса.
Не надо полагаться, что враг не нападет…

До участия в Первом Уральском форуме.

Работа по «классической» схеме:

- установка обновлений ПО (ОС, СУБД, веб-приложений);
- мониторинг «оперативной» информации о выявленных уязвимостях;
- тестирование обновлений АБС (технологические изменения);
- анализ сбоев и инцидентов;
- мониторинг информации об инцидентах в банковском секторе;
- стандартные проверки ИБ собственными силами.

Попыток хищения не было.

7 ЛЕТ. История вопроса.
Не надо полагаться, что враг не нападет…

Итог Первого Уральского форума.

Хищения через системы ДБО – не миф.

Почему это возможно:

- условия, способствующие хищениям;
- обсуждение существующих схем хищений;
- обсуждение возможного развития схем хищения.

Как предотвратить:

- противодействие имеющимися средствами;
- возможные направления развития средств защиты;
- организация системы оперативного оповещения;
- формулирование необходимых требований к защите системы ДБО;
- рекомендации по защите на стороне Клиента;
- рекомендации по защите от DDOS-атак.

7 ЛЕТ. История вопроса.
Не надо полагаться, что враг не нападет…

Практическая реализация.

Расширение функциональных обязанностей ИБ:

- самостоятельный анализ защищенности систем;
- использование сертифицированных СКЗИ;
- использование защищенных носителей ЭП;
- «разъяснительная» работа с Клиентами;
- фрод-мониторинг;
- межбанковское взаимодействие по предотвращению попыток хищений;
- «внешний» анализ защищенности систем;
- устранение выявленных уязвимостей в ПО АБС и ДБО.

Попыток хищений стало существенно меньше, но они всё еще есть.

ЧТО МЫ ИЩЕМ.
Чтобы построить крепкую стену, нужно знать все слабые места.

Типовая схема контроля уязвимостей

Объект контроля	Поиск	Устранение	Контроль
Человеческий фактор	Служба ИБ	Служба ИБ	Служба ИБ
Межбанковские приложения	Регулятор	Разработчик	Служба ИБ
Информационные потоки	Служба ИБ	Служба ИБ	Служба ИБ
Межсистемные приложения	Внешний аудит	Разработчик	Служба ИБ
Клиентские приложения	Внешний аудит	Разработчик	Служба ИБ
АБС	Внешний аудит	Разработчик	Служба ИБ
Системное ПО (ОС, СУБД, Web)	ИБ сообщество	Разработчик	Служба ИБ

КАК МЫ ИЩЕМ.
- Ты уязвимость видишь?
- Нет… ☹
- А она есть!!!

Как это работает на практике.

Необходимые условия:

- полное знание и документирование ИС;
- хороший аудитор;
- хороший разработчик;
- единое информационное пространство для совместной работы;
- мониторинг «внутренних и внешних» событий;
- анализ выявленных уязвимостей, их устранение и контроль;
- «стандартные» проверки ИБ;
- непрерывность процесса;
- наличие «рычагов воздействия».

КАК МЫ ИЩЕМ.
- Ты уязвимость видишь?
- Нет… ☹
- А она есть!!!

Как это работает на практике.

Единое информационное пространство для совместной работы.

Информационная безопасность

Проект	Код
Аудит ИБ	DSEC
Безопасность ДБО	SDBO
Мониторинг операций по картам	TWFA
Обслуживание СКЗИ	CRYPTO
Перспективные разработки ДКИ	DKING
Соответствие 152-ФЗ	PDN
Соответствие PCI DSS	PCIDSS
Соответствие СТО БР ИББС	IBBS
Управление учетными записями	USR
Управление уязвимостями	HACK

Информационные технологии

Проект	Код
Взаимодействие АБС	UNION
Межсистемное взаимодействие	EXCH
Процессинговый центр	NWPC

КАК МЫ ИЩЕМ.
- Ты уязвимость видишь?
- Нет… ☹
- А она есть!!!

Практические примеры.

Уязвимость на стороне Клиента.

- нет поддержки от разработчика;
- затратность предлагаемых «навесных» решений;
- «самописные» решения;
- «неудобство» дополнительных мер безопасности;
- актуальность средств «обратной» связи с Клиентом.

Защиту Клиента Банк вынужден обеспечивать самостоятельно.

КАК МЫ ИЩЕМ.
- Ты уязвимость видишь?
- Нет… ☹
- А она есть!!!

Практические примеры.

Уязвимость в технологии.

«Коробочное» решение и кастомизация:

- ошибки в архитектуре;
- «вечные» fix и patch;
- затраты на оборудование для тестирования;
- затраты на анализ защищенности;
- правильность реализации технологии;
- необходимость доказательства серьёзности уязвимости.

Возможно ли выполнение большей части этих работ на площадке разработчика, силами экспертной группы?

КАК МЫ ИЩЕМ.
- Ты уязвимость видишь?
- Нет… ☹
- А она есть!!!

Практические примеры.

Уязвимость в реализации решения. Всё проверили, но…

Человеческий фактор:

- формальное выполнение;
- check-list;
- возврат старых ошибок;
- режим восстановления;
- каждый раз полная проверка;
- база знаний.

Необходима четкая регламентация и контроль режима эксплуатации ИС.

КАК МЫ ИЩЕМ.
- Ты уязвимость видишь?
- Нет… ☹
- А она есть!!!

Практические примеры.

Уязвимость в информационных потоках.

Человеческий фактор:

- нарушение технологии;
- незначительная избыточность прав доступа;
- вынуждение к действиям;
- злой умысел.

Необходимо ли развитие анализа защищенности этого направления?

БАНК SIAB

ЗАЧЕМ МЫ ИЩЕМ.
Сделать нападение на себя невозможным.

Внутренняя потребность.

Анализ защищенности ИС дает нам возможность:

- проверить свои силы в режиме «реальной» атаки на ИС;
- проверить эффективность принимаемых организационных мер;
- проверить эффективность взаимодействия служб;
- предоставить Руководству независимую оценку уровня защищенности;
- учитывать экспертный опыт;
- получить экспертное заключение о соответствии требованиям.

Нам еще есть куда развиваться.

БАНК SIAB

ЗАЧЕМ МЫ ИЩЕМ.
Сделать нападение на себя невозможным.

Внешняя потребность.

Количество должно перейти в качество. Возможно ли это?

- единое доверенное информационное пространство;
- централизованное управление процессом;
- база инцидентов в режиме on-line;
- расширенная экспертная группа;
- help-desk и support;
- независимая оценка ТЗ, реализации, тестирования, модификации;
- работа на площадке разработчика;
- лучшие практики для самооценки защищенности.

Семь лет поиска дают надежду, что это возможно.

БАНК SIAB
Практичные решения для жизни

СПАСИБО ЗА ВНИМАНИЕ!

НИКИТИН А.В. NIKITIN@SIAB.RU

19.02.2015

УРАЛЬСКИЙ ФОРУМ