Эволюция в SOC

Романов Сергей | АКБ «Энергобанк» (ПАО)

Подход к созданию СОИБ, при котором система развивается в SOC. Опыт АКБ «Энегробанк» (ПАО)

Область проекта | Ограничения | Шаги | Проблемы | Сложности | Факторы успеха | Выводы | Уровни зрелости | Результаты | Тезисы

Область проекта по созданию СОИБ

- ***Ликвидация последствий инцидента.***
- Ликвидация технологического отставания от уровня кибер-преступников.
- Модернизация действующей системы обеспечения информационной безопасности.
- Соответствие законодательству.

Ограничения

- Время:
  - проверки ЦБ РФ(382-П и по манипулированию рынком), РКН(ФЗ-№152);
  - действующие ИТ проекты;
  - необходимость достижения допустимого уровня информационной безопасности до старта проекта;
  - планирование ресурсного обеспечения.
- Штат - не более 5 сотрудников.
- Исключенные цели – международный compliance.

Шаги

Название шага	Итог реализации
0. Определение цели.	**Цель – удовлетворение ожиданий заинтересованных сторон**(Акционеры, Высший менеджмент, клиенты, надзорные и регулирующие органы, клиенты, сотрудники, контрагенты).
1. Оптимизация имеющихся ресурсов для повышения уровня ИБ	Результаты аудита, список уязвимостей, безопасная конфигурация инфраструктуры, **повышение осведомлённости.**
2. Определение стратегии ИБ	**Стратегия: «ИБ – сервис!». Привлечение заинтересованных сторон,** формализованные ценности заинтересованных сторон, формализованные бизнес-процессы, действующие пилотные проекты средств защиты.
3. Реализация	**Экономическое обоснование**, закупка и внедрение, перенос конфигураций с пилотируемых решений.
4. Эксплуатация	**Преобразование сервиса**, решение проблем, снижение издержек.
5. Оценка результатов	**Факторы успеха, метрики эффективности, презентация результатов.**

Цитата: «Услуга – это процесс. Сервис – это результат! Продавайте именно Сервис, а не Услуги».

Проблемы и сложности

Шаг	Проблема/сложность	Решение/применяемые методы
Шаг 3	Экономическое обоснование	Формулировка бизнес-потребности, оценка соответствия, анализ рисков, использование математической модели сравнения решений, расчёт экономических показателей.
Шаг 4	Недостаточная квалификация сотрудников по: •эксплуатации приобретённых СЗИ; •расследованию кибер-преступлений; •Реагированию на инциденты; •аналитике.	Создание тестовой среды СЗИ. Строгая политика правил корреляции(повышенный % false-positive) . Реализация отклонений в соответсвии с бизнес-процессами.
	Штатная численность (уход специалиста)	Принятие рисков и согласование ограничений.
	Необходимость мониторинга 24 на 7	Автоматизация реагирования на инцидент, обратная реакция.

Факторы успеха

Удовлетворённость заинтересованных сторон:

- Акционеров – повышение степени непрерывности бизнеса(предоставлены результаты испытаний);
- Высшего менеджмента – соблюдение бюджета;
- Регулирующих и надзорных органов – успешное прохождение проверок РКН и ЦБ РФ;
- Клиентов – *находится на стадии оценки;*
- Контрагентов – отсутствие обращений;
- Сотрудников – отсутствие запросов на тех. поддержку и на повышение привилегий.

Пример KPI на основе факторов успеха

1. Число выявленных проверяющими нарушений.
2. Допустимое отклонение оценки соответствия.
3. Количество запросов сотрудников(повышение прав, уровня доступа).
4. Превышение бюджета на сумму.
5. Количество приостановок бизнес-процессов.
6. Количество приостановок сверх допустимого времени.
7. Количество обращений клиентов.
8. Количество инцидентов с материальными потерями клиентов.

Уровень зрелости системы как этап эволюции

- Этап 0 – «несуществующая». Появились цели.
- Этап 1 – «примитивная». Появилась безопасная конфигурация.
- Этап 2 – «начальная». Появилась стратегия развития.
- Этап 3 – «формализованная». Появилось ресурсное обеспечение и описание процесса.
- Этап 4 – «управляемая». Появились современные средства защиты и контроля, внедрена СМИБ.
- **Этап 5 – «оптимизированная, SOC».** Собраны оценки заинтересованных сторон.

Итоговые результаты

1. Действующий сервис по ИБ.
2. Автоматизированная обратная реакция.
3. Единая база каталогов и индикаторов компрометации.
4. Подключение к внешним источниками и глобальной репутации.
5. Процесс эффективного использования ресурсов.
6. Формализованные бизнес-процессы, в том числе и ИБ.
7. Эффективное управление ожиданиями заинтересованных сторон.
8. Становление ИБ продуктом, который можно продавать.
9. Согласованность подхода с ITIL, COBIT, ISO27000.

Тезисы

- Удовлетворите ожидания заинтересованных сторон.
- Любая система эволюционирует в SOC.
- SOC способен удовлетворить ожидания.
- ИБ – это сервис, а не услуга.
- Эффективное совершенствование системы не возможно без расчёта окупаемости и рентабельности.
- Оценивайте рентабельность с учётом возможного аутсорсинга – оптимизируйте ресурсы и минимизируйте ограничения.

Анонс. Вопросы?