НАЦИОНАЛЬНЫЙ БАНК КАЗАХСТАНА

Управление информационных угроз и киберзащиты

Партнерство служб ИТ и ИБ

Анатолий Пудель
2019

О чём доклад?

- С чего начать построение отношений между ИБ и ИТ
- Основные точки соприкосновения
- Как проявляется конфликт интересов и есть ли он?
- Практики по построению взаимоотношений

С чего новому CISO начать построение отношений между ИБ и ИТ

- Изучить орг. структуру и найти уровень на котором сходятся интересы ИТ и ИБ (общий куратор или общий руководитель отдела/департамента, первый руководитель компании, ИБ в составе ИТ)
- Составить функциональную карту (какие ИТ/ИБ процессы формализованы, границы ответственности подразделения ИБ)
- Изучить существующие договоренности об исполнении взаимных запросов (установленные возможности приоритезации, сроков исполнения различных видов запросов)
- Изучить имеющуюся базу инцидентов ИБ (фиксировались ли атаки, на какие активы)
- Изучить ИТ архитектуру компании
- Понять какие подходы по управлению ИТ процессами существуют

Основные точки соприкосновения ИТ и ИБ

- Управление ИТ активами (учет, оценка)
- Управление ИТ архитектурой
- Согласованность методологий ИТ/ИБ
- Управление доступом (аутентификация, администрирование, матрицы доступа)
- Жизненный цикл информационных систем
- Управления изменениями и конфигурациями
- Управление носителями данных
- Зависимость бюджетов ИТ/ИБ
- Журналирование событий и их анализ
- Реагирование на инциденты
- Обеспечение непрерывности бизнеса
- Управление внешними поставщиками (аутсорсинг)

В чем проявляется конфликт интересов и есть ли он?

Цели ИТ	Цели ИБ	Неверная цель для ИБ
обеспечить реализацию бизнес стратегии		закрутить гайки, чтобы не появлялись инциденты
обеспечивать соответствие ИТ-сервисов требованиям бизнеса	обеспечивать соответствие ИБ-сервисов требованиям бизнеса	заставить бизнес подразделения работать «безопасно»
соответствие требованиям регуляторов за приемлемые расходы		любой ценой исполнить регуляторные требования
управлять ИТ-рисками	управлять ИБ-рисками	исключить все риски ИБ
безопасность информации, приложений, инфраструктуры		

В чем проявляется конфликт интересов и есть ли он?

Как правило:
1. ИТ – основные ресурсы направляет на поддержку **доступности** ресурсов и реализацию проектов бизнеса
ИБ – на снижение рисков ИБ (конфиденциальность, целостность, **доступность**) при функционировании ИТ систем и реализации проектов

Следствие:
*обеспечение ИБ всегда требует **увеличения/дополнительных ресурсов** для сопровождения ИТ ресурсов*

2. При подчинении руководителя ИБ директору по ИТ или безопасности в компании нет стратегии развития ИБ, не проводятся эффективные коммуникации с высшим руководством по вопросам обеспечения ИБ, возможно умалчивание неудобных проблем, в том числе неисполнение требований регуляторов.

Следствие:
Для получения максимального эффекта руководитель службы ИБ должен подчиняться первому руководителю компании и иметь право голоса в необходимых коллегиальных органах

Практики по построению взаимоотношений

- Начните обсуждать с ИТ не технологии, а риски ИБ и их влияние на цели компании
- Планируйте совместные проекты (новые сервисы для бизнеса)
- Устанавливайте совместные KPI
- Составьте совместный план развития ИТ/ИБ на основании бизнес стратегии и доведите его совместно до работников ИТ/ИБ
- Добейтесь четкого разделения сфер ответственности там, где возможно
- Будьте честными друг с другом, доводите всю информацию которая имеет значение

Практики по построению взаимоотношений

- Выстраивайте доверительные и прозрачные отношения (общий доступ к системам аудита событий, единый учет инцидентов, совместная обработка заявок пользователей в service desk)
- Проводите перекрестное и совместное обучение персонала
- Обсуждайте ресурсные ограничения с участием кураторов/руководителей
- Совместно устанавливайте приоритеты задачам и управляйте ожиданиями
- Найдите мотивированных работников для продвижения и улучшения климата между службами
- Проводите регулярные встречи ИТ и ИБ
- Предложите ИТ использовать SIEM для мониторинга инфраструктуры
- Совместно доводите до высшего руководства недостатки ИБ в инфраструктуре
- **Сделайте все, чтобы у ИТ были ресурсы для минимизации рисков ИБ!**

Спасибо за внимание!

Анатолий Пудель
начальник Отдела предотвращения информационных угроз Национальному Банку
Управления информационных угроз и киберзащиты
Национального Банка Республики Казахстан, CISM
anatoliy.pudel@nationalbank.kz