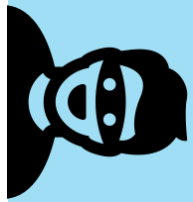


Управление инцидентами в антифроде

Система антифрода выявила фрод.
Что дальше?!

Дмитрий Бергер
d.berger@cft.ru

Реактивный подход к инцидент-менеджменту

Что-то произошло

Действуем

Успокоились

Наш план

1. **Задачи и общая структура процесса**
2. **Детали процесса**
3. **Несколько важных аспектов**

Задачи инцидент-менеджмента

- Обработка в плановом режиме
- Отвлечение минимально достаточных ресурсов
- Минимум негативного влияния
- Извлечение уроков
- Информированность сторон

Структура процесса

Тушим пожар

Обрабатываем

Извлекаем опыт

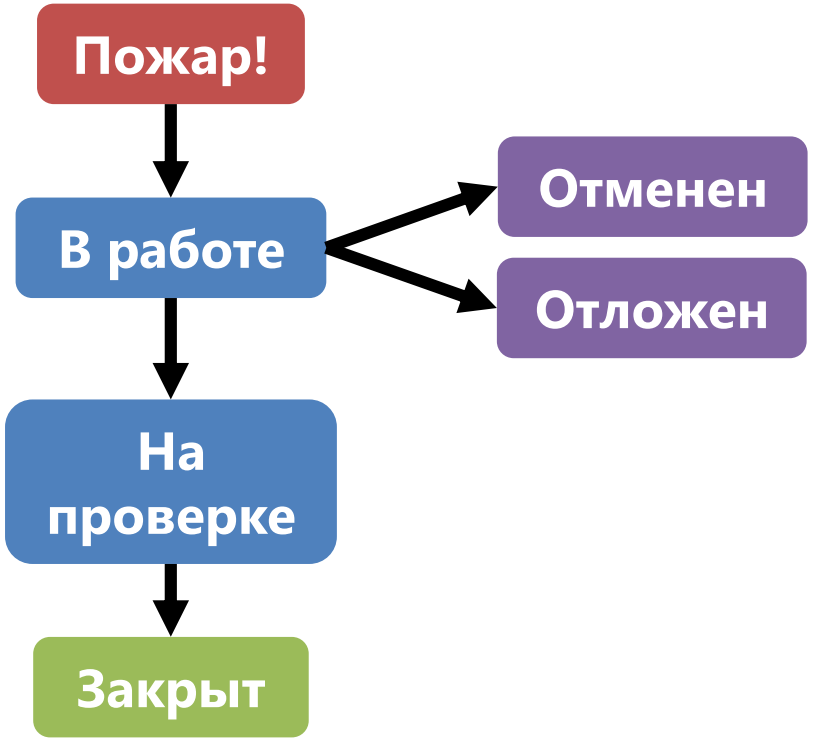
Прокачиваем процесс

Тушение пожаров

- Инструкции у всех сотрудников
- Дежурные на всех периметрах
- Информирование всех
- Оценка масштаба
- Оценка приоритета
- Локализация проблемы

Регламент обработки

- Проект в Atlassian Jira
- Специальные рабочие столы
- Строгий Workflow
- Подробная система классификации
- Автоинформирование заинтересованных
- Отчетность



Обработка инцидента

- Расследование
- Владелец
- Рабочая группа
- План и ответственные
- Информирование
- Детализация и документирование

Критичность инцидента

Обычный

Высокий

Блокирующий

Извлекаем уроки

- Как мы могли предотвратить инцидент?
- Как мы могли снизить потери?
- Какие ошибки допустили при обработке?
- Как мы могли заметить инцидент раньше?
- Каких инструментов нам не хватает?

Прокачка и модернизация

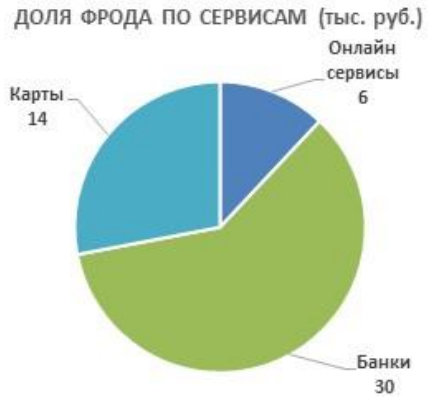
- Технологии
- Процессы
- Обучения
- Информирование
- Открытость

Информирование ФинЦЕРТ

Прозрачность процесса

ЕЖЕНЕДЕЛЬНЫЙ ОТЧЕТ ПО БЕЗОПАСНОСТИ

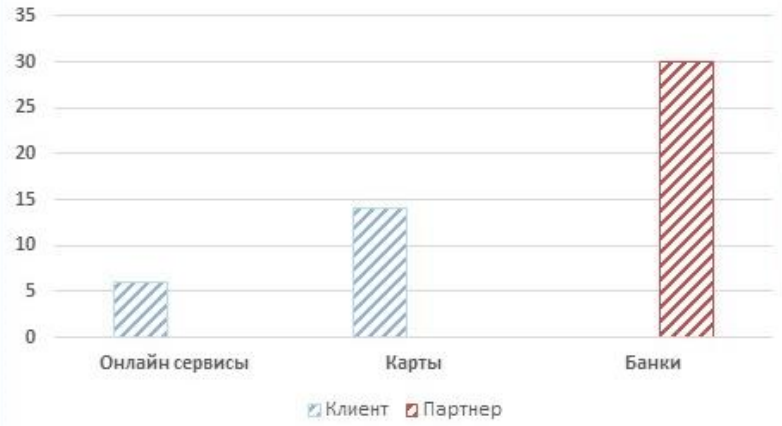
2 МАРТА – 8 МАРТА



ВАЖНЫЕ СОБЫТИЯ ОТЧЕТНОГО ПЕРИОДА

- Мошенники за прошедшую неделю вывели 5 тыс. руб. с карт клиентов сторонних банков транзитом через онлайн сервисы «Бронзовый перстень». Большая часть денежных средств была приостановлена и возвращена пострадавшим Клиентам. Ущерб составил 1 тыс.руб. Мошеннические реквизиты внесены в ЧС.
- В результате социальной инженерии 6 Клиентов разгласили данные по картам и одноразовые коды для подтверждения списания ДС с карт. Платежи были приостановлены антифрод системой. Спасено 14 тыс.руб. Мошеннические реквизиты внесены в ЧС.
- Мошенники позвонили в отделение банка «Зеленый Крокодил» и с помощью социальной инженерии убедили оператора банка совершить платеж на реквизиты карты «Чебурашка» Банка без внесения ДС в кассу. Операция была приостановлена антифрод системой и денежные средства в полном объеме (30 тыс.руб.) были возвращены на р/счет пострадавшего Банка. Мошеннические реквизиты внесены в ЧС. Усилены правила антифрод системы.

ПОТЕРПЕВШИЕ СТОРОНЫ



партнер — 30 тыс.руб.

клиент — 20 тыс.руб.

Источники событий

- Фрод-мониторинг
- Обращения клиентов
- Запросы правоохранительных органов
- Интернет, СМИ
- Анализ отклонений
- Сигналы от партнеров

Дмитрий Бергер
d.berger@cft.ru