SOC
FORUM
2023

Построение ИБ с нуля – практический опыт и рекомендации

МОСКВА 2023

SOC
FORUM
2023

Васильев Александр Андреевич

АО «Невский экологический оператор»

SOC FORUM 2023

- Цели и задачи построения ИБ
- С чего начать построение ИБ и что обязательно нужно учесть
- Обоснование бюджета и дальнейшее развитие

Начало всего пути. Какие проблемы?

Начало пути. Какие проблемы?

SOC FORUM 2023

Главный вопрос в том, как объяснить в чем надобность создания ИБ?

1. Защита общества: при отсутствии ИБ может быть приостановлена работа всей организации

2. Требования действий организации в рамках федеральных законов (152-ФЗ)

Начало пути. Какие проблемы?

SOC FORUM 2023

- Неясное представление о рисках и угрозах
- Отсутствие базовых политик ИБ
- Ограниченный бюджет и ресурсы
- Недостаток осведомленности среди сотрудников

Задачи. Путь становления

Задачи. Путь становления

SOC FORUM 2023

2021

Запуск и оценка текущего состояния

2022

Усиление безопасности и соблюдение стандартов

2023

- Укрепление ИБ и обучение персонал
- Проведение аудита по ИБ
- Начало внедрения средств защиты

Задачи. Путь становления

SOC FORUM 2023

Развитие и внедрение средств защиты

2024

Улучшение, оптимизация, поиск новых средств применения защиты

2025

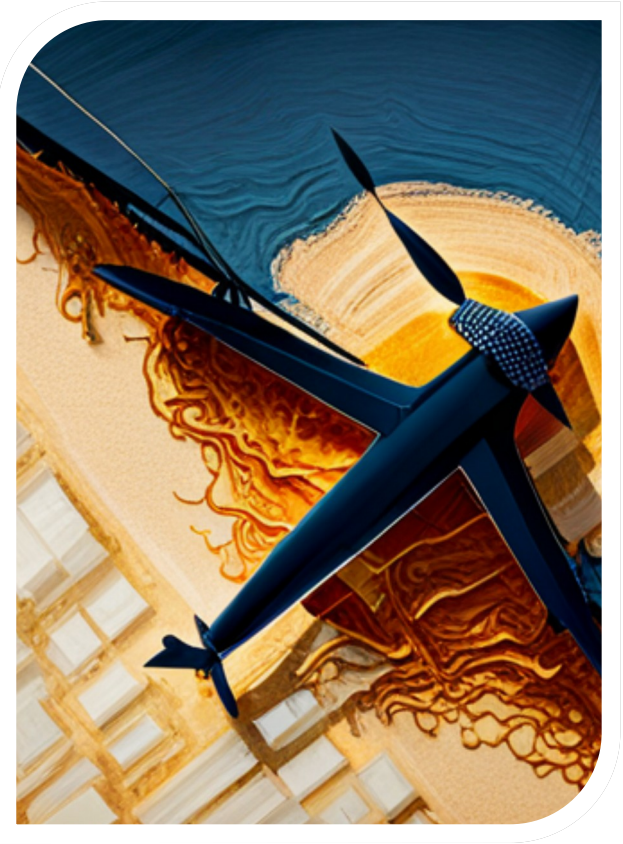
С чего начать построение ИБ и что обязательно нужно учесть

С чего начать построение ИБ и что обязательно нужно учесть

SOC FORUM 2023

Построение информационной безопасности (ИБ) следует начинать с:

- анализа рисков
- определения целей и задач
- разработки стратегии безопасности и внедрения соответствующих мер



С чего начать построение ИБ и что обязательно нужно учесть

SOC FORUM 2023

Важным моментом является четкое объяснение и обоснование надобности создания ИБ:

- Какие штрафы предусмотрены за нарушение законодательства
- Формирования понимание у коллег, что такое ИБ
- Примеры ошибок, которые допускают сотрудники, какие риски для общества

Самостоятельное исправление найденных уязвимостей

SOC FORUM 2023

Найденная уязвимость – это недостаточная аутентификация

ПРОБЛЕМА

Отсутствие верификации заявок на смену пароля пользователей. Администраторы направляли новые пароли без проверки подлинности запросов.

РЕШЕНИЕ

- Введение верификации пользователя с использованием карточек сотрудников
- Каждому сотруднику была выдана карточка в системе
- Номер, указанный в заявке, сравнивался с данными на карточке
- При совпадении номеров считалось, что верификация прошла успешно

Обоснование бюджета и дальнейшее развитие

Обоснование бюджета

SOC FORUM 2023

№	ПОЗИЦИЯ	ОБОСНОВАНИЕ ДЛЯ БИЗНЕСА
1	Построение системы защиты ПДн с учетом требований по импортозамещению	Показали штрафы за нарушение 152-ФЗ, а так же нормативные документы в администрации СПб. Объяснили риски
2	Проведение тестирования на проникновение	Показали и объяснили риски (несанкционированный доступ, утечка данных, повреждение репутации) При успешном использовании слабых мест хакером предусмотрена административная и уголовная ответственность Показали штрафы
3	Внедрение NGFW	Оборудование для блокировки атак хакеров из интернета. Показали и объяснили риски (Потеря конфиденциальных данных, повреждение репутации, замедление работы сети)
4	Внедрение сервиса WAF и AntiDDos	Сервисы, которые помогут защитить сайт предприятия и защитить доступ в интернет и к информационным системам. Показали и объяснили риски (потенциальные атаки на сетевую инфраструктуру, потеря конфиденциальных данных, повреждение репутации, финансовые убытки, замедление работы сети)
5	Обучение основам киберграмотности и безопасного использования ИТ-ресурсов для сотрудников	Рассказали про халатность сотрудников, объяснили какие риски это несет

Согласование и обоснование бюджета

SOC FORUM 2023

ФОРМИРОВАНИЕ БЮДЖЕТА

- Требовалось составить дорожную карту внедрения средств в ИБ

РЕШЕНИЕ

- Вместе с партнером провели анализ, удалось снизить затраты на 70%

ЗОНА ПОКРЫТИЯ

- ИСПДн;
- Политики и регламенты;
- Стратегическое и тактическое планирование

ДЕТАЛИ ПРОЕКТА

- Выбор и внедрение технических и организационных мер безопасности

Отражение атаки

SOC FORUM 2023

РЕЗУЛЬТАТЫ

Отражение спам-атаки и повышение защищенности;

Дополнительное доказательство в необходимости развития ИБ

ПРОБЛЕМА

- Злоумышленниками была инициирована атака, которая затруднила работоспособность некоторых управлений

РЕШЕНИЕ

- С помощью совместного анализа входящих писем удалось определить формат атаки и предотвратить атаку с помощью перенастройки правил

Фишинговые письма

Опыт с SOLAR

SOC FORUM 2023

ПРОЕКТ

Аудит по ИБ

РЕЗУЛЬТАТЫ

Анализ фишинговых писем и определение их реального источника

Дополнительное доказательство в необходимости развития ИБ

ПРОБЛЕМА

- Злоумышленниками были направлены фишинговые письма с поддельной информацией

РЕШЕНИЕ

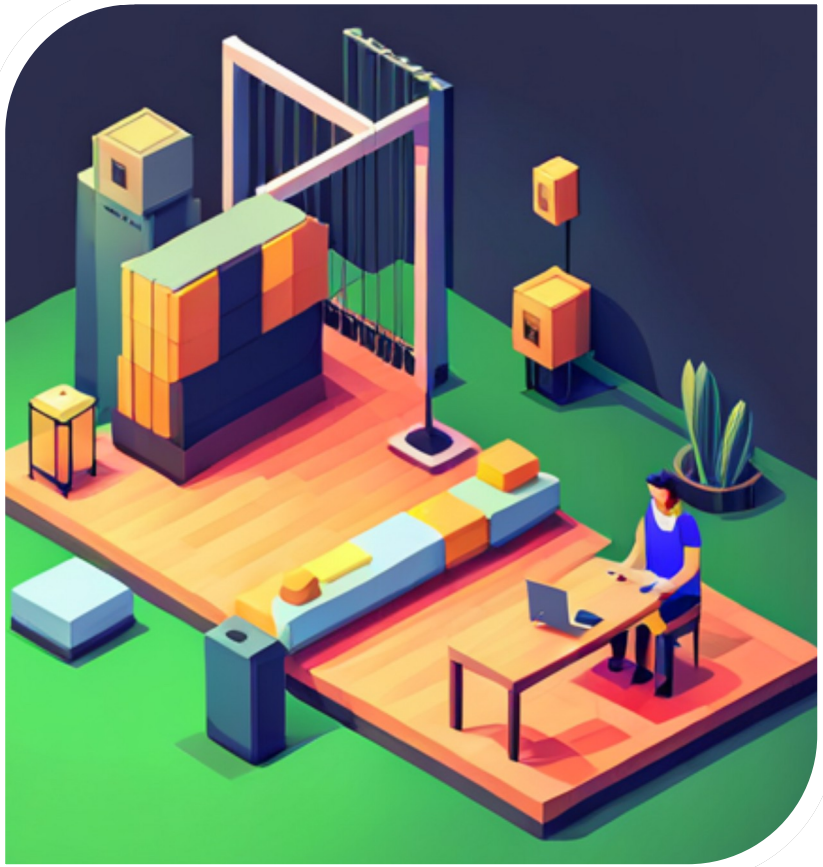
- С помощью Solar-Aura был выявлен реальный отправитель, с кем он был связан

Дальнейшее развитие ИБ

SOC FORUM 2023

Для дальнейшего развития информационной безопасности в Обществе необходимо:

- Регулярный анализ рисков и обновление стратегии безопасности
- Внедрение новых технологии и мер защиты
- Обучение и повышение квалификации сотрудников в области ИБ
- Осуществление мониторинга и аудита информационных систем



SOC FORUM 2023

Санкт-Петербург,
ул. Арсенальная д.1, к.2,
лит. А, офис 113
БЦ "Арсенальный"