

Киберзащита цифровой стройки

BIM, IoT и AI меняют стройку — кибербезопасность становится частью цифрового фундамента

Устюжанин Андрей

заместитель директора информационной безопасности

1

Стройка стала цифровой | Данные становятся частью фундамента

2

Новый риск | Атака доходит до физического объекта и до людей

3

Где и как бьют | Точки входа, BIM, стройплощадка, цепочка поставок

4

Реалистичные сценарии | Как атака складывается из уязвимостей

5

Что делать | Принципы защиты и с чего начать — по своей зрелости

Цифровизация стройки = работа с данными как строительство цифрового фундамента объекта

Цифровая стройка — это огромная распределённая ИТ-инфраструктура.

ИНТЕЛЛЕКТУАЛЬНЫЕ ДАННЫЕ

BIM-модели, расчёты, генерации идей, концепты проектов и решений

ДАННЫЕ ТЕХНИКИ И РОБОТИЗАЦИИ

Автономная техника, дроны для аэросъёмки, IoT-датчики бетона, цифровые геодезисты

ДАННЫЕ ЭКСПЛУАТАЦИИ И УПРАВЛЕНИЯ ДОМОМ

Умное здание: ОВК, лифты, доступы, видеонаблюдение, счётчики

ПЕРСОНАЛЬНЫЕ ДАННЫЕ

Данные сотрудников, жильцов, контрагентов

КОММЕРЧЕСКИЕ ДАННЫЕ

Информации о сделках, ценообразовании, скидках, продажи

Раньше кибер атака затрагивала и ломала системы. Сегодня она доходит до объекта строительства и людей

Это уже не вопрос ИТ, а вопрос безопасности объекта.



ПОСЛЕДСТВИЯ

Риск для безопасности и жизни. На кону не просто данные – жизни людей

У атаки нет одной двери: вход есть на каждом этапе жизненного цикла строительства

На каждом этапе — свои риски и своя тяжесть последствий. Слабое звено может быть где угодно.

1

Старт проекта

Фишинг, инсайдер, ранняя утечка замысла

2

Проектирование

Искажение расчётов, исходных данных, допустимых нагрузок, блокировка доступа, шифрование данных

3

Строительство

Искажение работы техники и информации с датчиков, предоставление несанкционированного доступа

4

Эксплуатация

Перехват управления умного здания, трансляция или продажа информации о жителях, подмена состояния оборудования

СКВОЗЬ ВСЕ ЭТАПЫ: ERP, СОД / CDE, ИСУП — единый цифровой слой над всеми данными

ПОВЕРХ ВСЕГО: Искусственный интеллект: генеративный дизайн, прогноз сроков, оптимизация — новый слой ценности и новый вызов (отравление данных, ошибки генерации)

«Умное» железо на стройке — это компьютеры с моторами. И ломают их как компьютеры

Защита площадки — отдельная инженерная задача, не похожая на защиту офиса

Краны и тяжёлая техника

Радиоканалы управления уязвимы для перехвата и подмены команд — не обязательно быть рядом.

IoT-датчики

Подмена показаний бетона и нагрузки нарушает технологию — скрытые дефекты конструкции.

Дроны

Перехват аэросъёмки — шпионаж за площадкой, ваш дрон становится оружием в чужих руках.

Автономная техника

Экскаваторы, 3D-принтеры зданий: атаки на каналы управления и систему позиционирования.

Видеонаблюдение

Камеры с заводскими паролями самая частая дверь во внутреннюю сеть площадки.

Личные устройства прорабов

Телефоны и ноутбуки, через которые ходят документы, фото и доступы.

Атакуют не вас. Фокус на слабое звено, у которого есть доступ к вам

Безопасность цепочки = безопасность слабейшего звена — и это ваша зона ответственности

Проектное бюро

доступ к моделям и СОД

Поставщики

доступ к спецификациям

Субподрядчики

доступ к ИСУП и площадке

Аренда техники

связь с диспетчерской

Облачная СОД

хостинг всех моделей

ИТ-сервисы и ПО

доступ в корпоративную сеть

▼ у всех имеются «живые» учётные записи в ваших системах ▼

ВАША КОМПАНИЯ — ГЕНПОДРЯДЧИК / ДЕВЕЛОПЕР

Взлом любого звена = вход в вашу инфраструктуру «как свой». Никто не отличает его от легитимного участника

Через маленькое бюро — в большой проект

Реальная реконструкция, типичная для отрасли

1 · ВХОД

Заражение подрядчика

Маленького подрядчика берут фишингом. Своей службы ИБ у него нет.

2 · ЗАКРЕПЛЕНИЕ

Вход «как свой»

Через учётку подрядчика — в общую среду проекта. Никто не отличает от легитимного.

3 · КРАЖА

Выкачка данных

Тихо забирают документацию: финансовые данные, модели, сметы, договоры.

4 · ШИФРОВАНИЕ

Проект тормозит

Шифруют общие ресурсы. Сначала украсть, потом зашифровать — двойная схема.

5 · ДАВЛЕНИЕ

Шантаж

Угроза опубликовать украденное — рычаг, чтобы заставить заплатить.

Через CRM — к клиентам и продажам

Реальная реконструкция, типичная для отрасли

1 · ВХОД

Компрометация сотрудника

Менеджер по продажам открывает фишинговое письмо или использует скомпрометированный пароль.

2 · ЗАКРЕПЛЕНИЕ

Вход в CRM

Получение доступа к базе клиентов и истории сделок, скидок и стоимости

3 · КРАЖА

Выкачка данных

ФИО, паспорта, телефоны, адреса, история обращений, условия сделок,

4 · ШИФРОВАНИЕ

Блокировка доступов

Шифруют общие ресурсы и доступ к исправлению ситуации

5 · ДАВЛЕНИЕ

Шантаж

Угроза опубликовать украденное — рычаг, чтобы заставить заплатить

Цифровая стройка ≠ безопасная стройка

Защита — неотъемлемая часть управления качеством, сроком и безопасностью объекта

1

**Изменился
характер риска**

Угроза теперь
доходит до
физического объекта
и до людей

2

ИБ — это база

Безопасность —
часть ценности
девелоперского
продукта, а не
«доделаем потом»

3

**Это общая
ответственность**

Слабое звено в цепочке
открывает весь проект.
ИБ касается всех
участников

4

Защита окупается

Предотвратить кратно
дешевле, чем устранять

ЗАЩИТА ПЛОЩАДКИ

Отдельная инженерная задача, не похожая на защиту офиса

Считать в деньгах не обязательно — достаточно перечислить потери

ОПЕРАЦИОННЫЕ

- Простой объекта и срыв сроков
- Штрафы по контрактам
- Повторная экспертиза проекта
- Сверхурочные на восстановление

ПРАВОВЫЕ И ФИНАНСОВЫЕ

- Ответственность за утечку ПДн
- Обратные штрафы регулятора
- Расходы на расследование
- Претензии и иски заказчика

СТРАТЕГИЧЕСКИЕ

- Репутация перед рынком и банками
- Утрата уникальных решений
- Доверие дольщиков
- Уход клиентов к конкурентам

БЕЗОПАСНОСТЬ — НЕ ЗАТРАТА, А ЦЕННОСТЬ

Предотвратить инцидент кратно дешевле, чем устранять последствия и восстанавливать

Безопасность выстраивают как фундамент для получения конкурентного преимущества

КЛЮЧЕВЫЕ ОПОРЫ

1

Выстроить с дизайна

Защита — критерий выбора платформы и подрядчика «из коробки», а не патч поверх. Это и есть «фича, а не баг».

2

Защитить источники данных

Версии с цифровой подписью и ролевой доступ: подрядчик-электрик видит свой раздел, а не всю модель и сметы.

3

Заккрыть цепочку

Требования ИБ в контрактах, чек-лист при подключении партнёра, вовремя гасить доступы ушедших.

4

Люди

Большинство инцидентов начинается с человека. Обучение и тренировки — процесс; и сотрудников, и подрядчиков.

5

Бэкапы с проверкой восстановления

Изолированно и регулярно. Шифровальщик на BIM-сервер — тестируйте восстановление.

С чего начать?

Даже частичное внедрение заметно снижает риск.
Полное — делает безопасность вашим конкурентным преимуществом

Базовая гигиена | MFA, бэкапы, закрыть забытые доступы, обучение фишингу.



Зрелые процессы | Ролевой доступ к моделям, чек-листы подрядчиков, мониторинг, план реагирования



Зрелая защита | SOC или партнёр, пентесты, управление уязвимостями, комплексные киберучения на объекте или организации

Благодарю за внимание

информационная безопасность
фундамент киберустойчивости

