Совместная защита IoT всеми участниками рынка

Андрей Дугин

МТС

Ты знаешь, что можешь!

Бизнес-ожидания от IoT

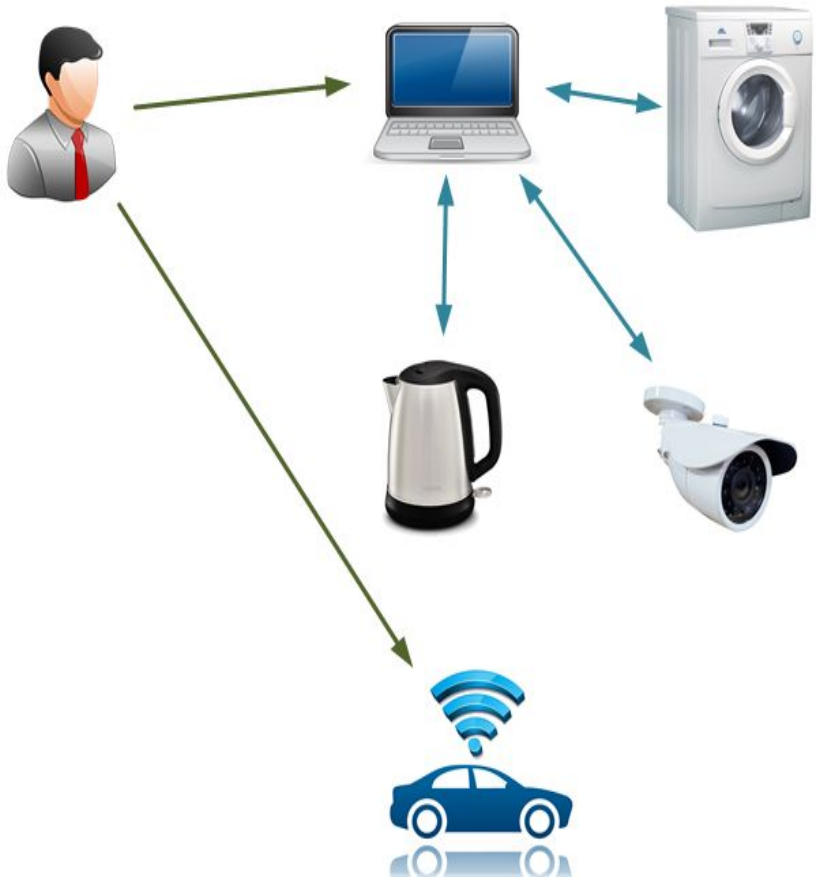
- Простота и удобство
- Имидж
- Автоматизированный сбор данных с физических объектов
- Контроль удаленных объектов без участия человека
- Сбор всей информации обо всем
- Входные данные для BigData
- Прогнозирование/предсказание событий
- Создание самоорганизуемых систем
- Монетизация

Угрозы компрометации IoT

- Нарушение неприкосновенности личной жизни
- Угроза жизни/здоровью
- Угроза физическому объекту
- Потеря контроля физического объекта
- Искажение собираемых данных
- Вымогательство
- Нарушение работы самоорганизуемых систем
- Организация площадки для атаки

Объекты защиты IoT

- **Устройства IoT**
  - Операционная система
  - Прикладная часть
  - Интерфейс управления
  - Интерфейс взаимодействия устройств
- **Система управления**
  - Операционная система
  - База данных
  - Прикладная часть
  - Интерфейс пользователя
  - Интерфейс управления устройствами IoT
- **Канал управления устройством**
- **Канал взаимодействия устройств**



Методы защиты IoT

Объекты защиты	Методы защиты
Устройства IoT	• Контроль целостности системных файлов • Резервное копирование • Контроль изменения конфигурации • Контроль уязвимостей • Управление обновлениями • Парольные политики
Система управления	
Канал управления устройством	• Выделение отдельного сегмента сети • Контроль доступа в сеть • Криптографическая защита
Канал взаимодействия устройств	

Участники рынка IoT

- Регулятор
- Производитель
- Интегратор решений
- Оператор связи
- Потребитель

Совместная защита IoT

- **Регулятор**
  - Определение правил игры для участников рынка
- **Производитель**
  - Внесение в инструкцию по эксплуатации памятки о мерах ИБ
  - Контроль безопасности кода ПО
  - Тестирование безопасности устройств и приложений
  - Поддержка работы в безопасной архитектуре
  - Безопасная конфигурация устройств
  - Принудительная смена пароля по умолчанию, парольные политики
  - Автоматическая проверка критичных обновлений
  - Удобное оповещение о необходимости обновления
  - Простой и быстрый процесс обновления ПО

Совместная защита IoT

- **Интегратор решений**
  - Разработка безопасной архитектуры для потребителя
  - Безопасная конфигурация компонентов решения
  - Документирование решения
- **Оператор связи**
  - Выделение канала
  - Сегментация сети, правила межсегментных взаимодействий
  - Контроль доступа в сеть
  - Контроль полосы
- **Потребитель**
  - Определение требований ИБ
  - Контроль соблюдения требований ИБ поставщиком и интегратором
  - Соблюдение рекомендаций производителя/интегратора по ИБ

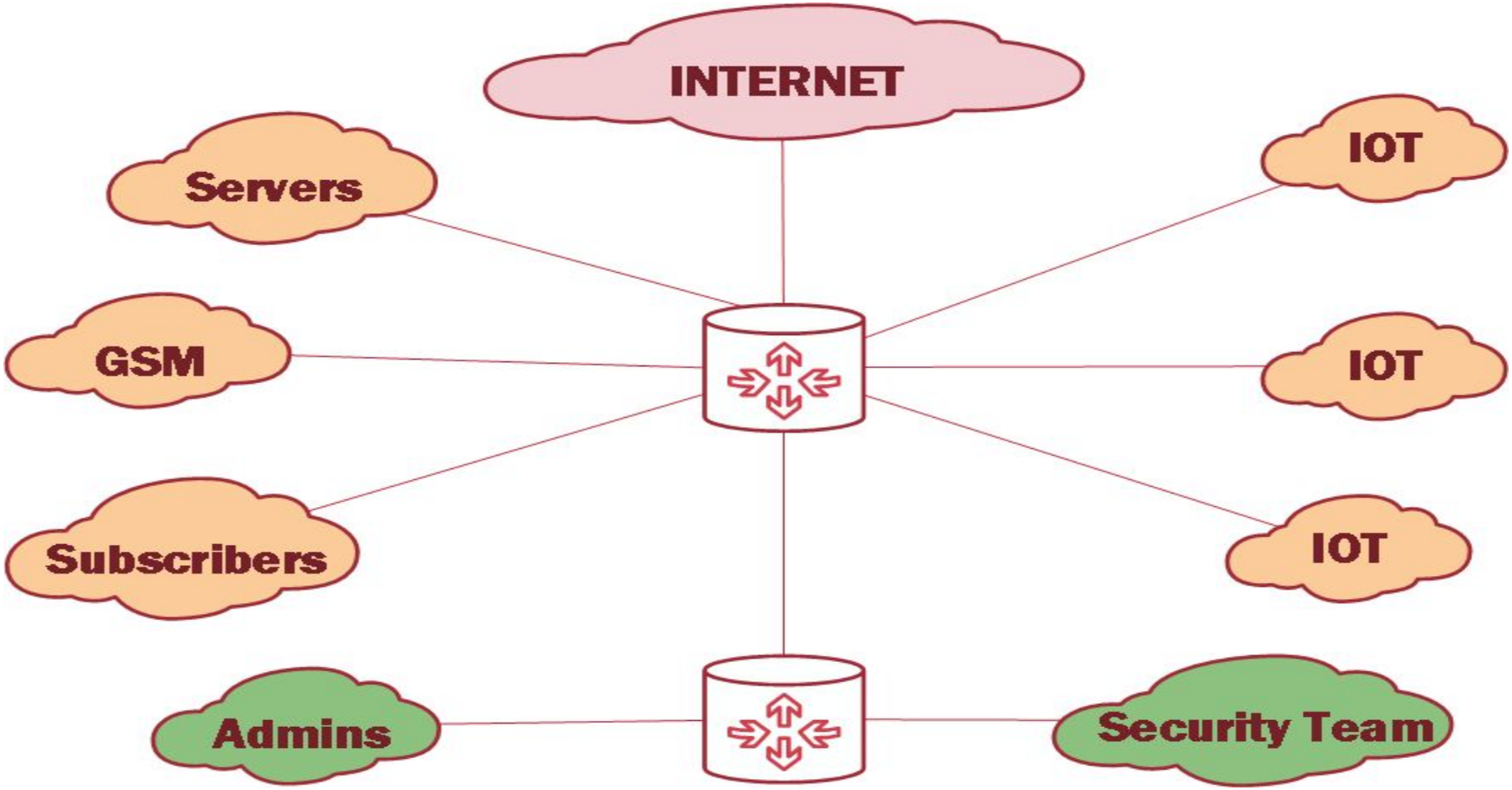
Защита IoT оператором связи. Тестирование под атакой

Телеком-защита IoT

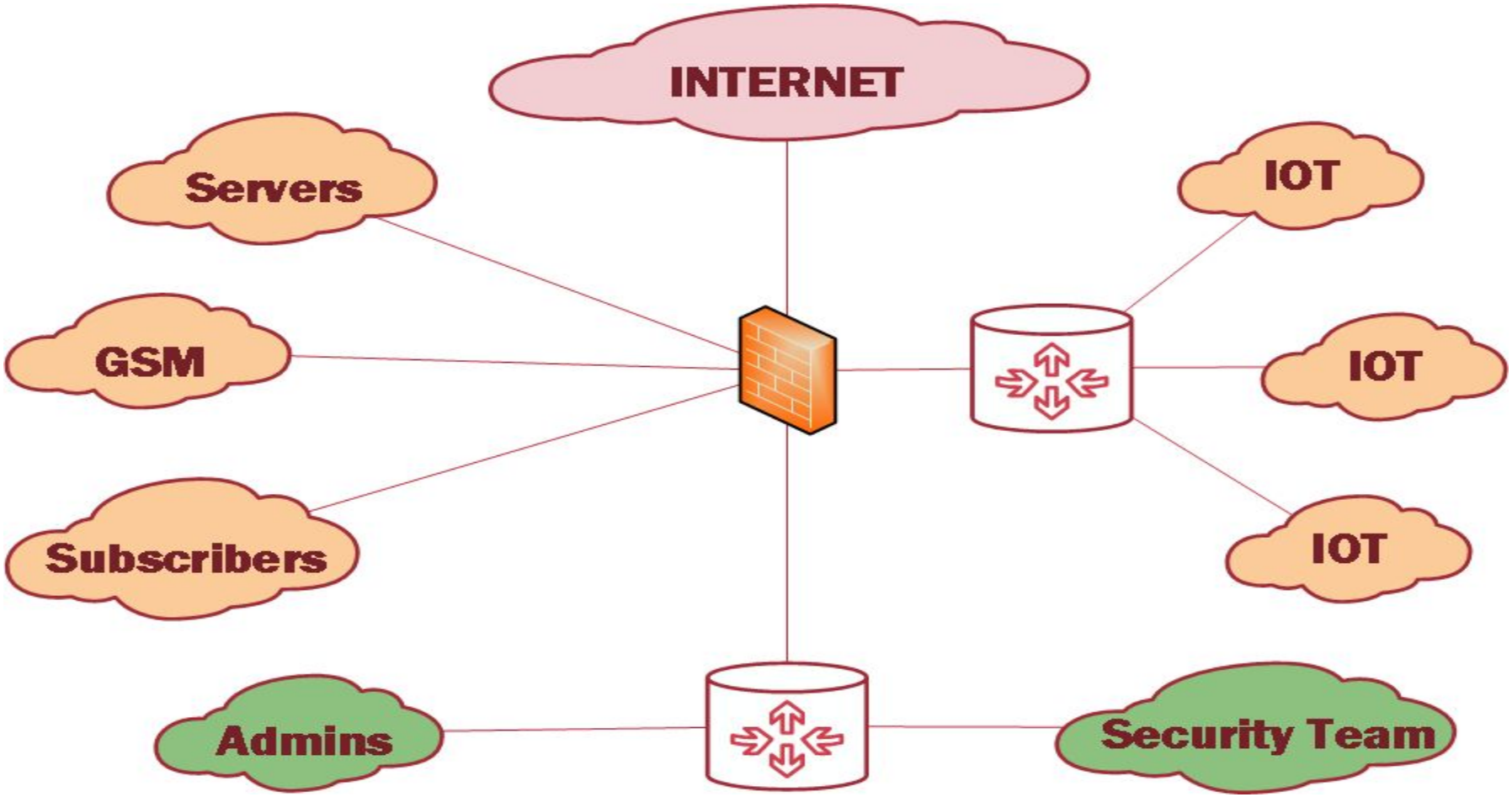
Positive Hack Days VII Противостояние (The Standoff) 2017

- **Исходные данные:**
  - 28 часов непрерывных атак 23-24 мая 2017
  - 6 защищаемых сегментов (из них 3 – IoT) и IP/MPLS-сеть
  - Более 100 защищаемых устройств
- **Реализованные меры:**
  - Разработка и реализация защищенной архитектуры
  - Объединение сегментов IoT, защита с помощью firewall и IPS
  - Контроль межсегментных взаимодействий
- **Результат: IoT не был взломан**

Телеком-защита IoT – изначальная схема



Телеком-защита IoT – безопасная схема



Q&A

Спасибо!

МТС

Ты знаешь, что можешь!