О защите корпоративных устройств для удаленного доступа

Проблематика

- Вектора атак
  - Фишинг
  - Использование личных/нерабочих интернет-ресурсов
  - Атаки на цепочки поставок или разговор про доверие
- Используемое оборудование, ПО
  - Полномочия пользователей в системе
  - Внешние носители ОС
  - Специализированные терминальные системы
  - Патчинг ОС, ПО
  - Предустановленные СЗИ
  - BYOD
- Возможности взаимодействия с корпоративной средой
  - Обмен файлами
    - Буфер обмена для RDP сессий
    - Облако
    - Мессенджеры, ВКС
    - Электронная почта
    - VPN клиенты
  - Проброс видео и звука
- Кибергигиена
  - Хранение логинов и паролей от учетных записей в легкодоступных местах
    - Сохранение паролей в браузерах, клиентах RDP и т.п.
    - Автологон
    - SSO
  - Использование единых паролей для доступа к корпоративным и личным ресурсам
  - Подключение к общедоступным wifi точкам и сетям
- Опубликованные корпоративные ИТ-сервисы
  - Каждый опубликованный в интернет сервис - потенциальная угроза безопасности и точка входа для злоумышленника

Подходы к решению

- Тчательная настройка среды для удаленных подключений и подготовка пользовательского оборудования
  - Принцип необходимости и достаточности
    - Корпоративные образы в режиме киоска
  - Управление временем доступности ИТ-сервисов
  - Гранулированный доступ к корпоративным ИТ-сервисам и ресурсам
  - Настройка VPN подключений
  - Биометрия и использование нескольких факторов для аутентификации
- Security Awarness
- Реагировать или недопускать - несколько слов про превентивность
- Автоматизация детектирования и реагирования
  - Реагирование 24x7 за счет СЗИ
  - Достаточно информативная система оповещений об инцидентах ИБ на случай отсутствия круглосуточного мониторинга
- Про вероятность и управляемость