"Кто же на самом деле контролирует твою инфраструктуру?"

Михаил Кадер

Архитектор по информационной безопасности

Удаленный доступ как неизбежная реальность

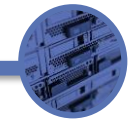
- Пандемия
- Экономия
- Цифровые бедуины

Взаимодействие и риски

Удаленное рабочее место

Взаимодействие – Устройства/Пользователи к приложениям и Администраторы для управления ими

Риски – Недостаточная осведомленность, незащищенные соединения, нарушения политик, уязвимости, ВПО, взлом



Приложения

Итак, кто же контролирует твое рабочее место?

- Я!
- Администратор
- Друг
- Враг
- Враг друга
- Друг врага
- Враг врага
- И т.п.

А что хотелось бы?

- Избежать нарушения работоспособности
- Избежать хищения данных
- Избежать компрометации корпоративной инфраструктуры
- Избежать компрометации корпоративных приложений
- И прочее по вкусу

Защитные средства

Анти …. и E(X)DR

- Защита от всяческих взломов и хищений, в том числе с использованием соц. инженерии
- Эффективный
- Не навязчивый
- Управляемый
- Интегрированный с другими средствами защиты (X)

Клиент VPN

- Постоянное соединение
- Интеграция с многофакторной аутентификацией
- Управляемый
- Не надоедливый ☺

Шлюз VPN

- Телеметрия
- Ролевое ограничения сетевого доступа
- Производительность и надежность (кластеры, распределение нагрузки, облака, расположение)

AAA и т.п.

- Интеграция с корпоративным каталогом пользователей
- Возможность передачи на шлюз VPN ограничений по сетевому доступу на основании политик
  - Местоположение
  - Рабочие часы
  - Должностные обязанности
  - Типы устройств
  - Количество подключений
  - Может еще что в голову придет

Сетевая безопасность

- Трансляция ограничений доступа на инфраструктуру ИТ
  - VLAN
  - VXLAN
  - Фильтры
  - МСЭ
  - Виртуальные среды
  - Телеметрия

Поведенческая аналитика

- Для нее то нам и нужна телеметрия
  - Клиенты
  - Шлюзы VPN
  - Сетевая инфраструктура
  - Сервера AAA/MFA
  - И прочее
- Взломы удаленных пользователей
- Взломы ИТ систем
- Злонамеренное поведение
- «Плохие» протоколы и приложения
- Ошибки настроек сетевого доступа и безопасности

А можем ли мы все сделать сами?

- В целом, почему бы и нет?
  - Персонал, его квалификация и количество
  - Доступность и качество технических средств
  - Полнота технического решения
  - Документация
  - Политики
  - Эксплуатация ;-(
  - SOC? Свой? Услуга?

Мои выводы

- Реализовать надежный защищенный удаленный доступ – не «бином Ньютона»
- Определите исполнителя на этот процесс
- Обращайте внимание на удобство пользователей
  - Постоянный VPN
  - Удобный MFA
  - Не шумная защита от ВПО/EDR
- Ролевое управление доступом для уменьшения поверхности атаки
- Поведенческая аналитика расскажет о проблемах/инцидентах
- Дашбоард ;-)

Ваши вопросы?