Кибербезопасность: сохранение ИТ-инфраструктуры. Что нужно учесть, чтобы обеспечить защиту бизнеса?

МегаФон

Станислав Погоржельский

Руководитель по технологической поддержке
облачных и инфраструктурных решений

МегаФон

Какие темы мы с вами обсудим?

- Применение инструментария сотрудника ИБ на примере кейса
- На что должен руководитель компании обратить внимание
- Бонус! Чек-лист задач, которые помогут Вам понять точки уязвимостей вашей ИТ инфраструктуры и аналитика КБ от МегаФон

МегаФон

Кибератаки-2022

С марта наблюдается кратный рост кибератак на российские организации

×9,6

Увеличилось количество атак на инфраструктуру клиентов

×5

Увеличился спрос на сервисы кибербезопасности

МегаФон

Тренд на кибербезопасность

Спрос определяется двумя драйверами: нехваткой оборудования и человеческих ресурсов для быстрой адаптации к новым условиям

Исследование МегаФона

Кибербезопасность перестала быть вопросом только лишь соответствия требованиям регуляторов. Теперь информационная безопасность — одно из основных средств достижения бизнес-целей.

25%
Государственные учреждения

72%
Новых клиентов представляют коммерческие организации

3%
СМИ

МегаФон

Какова цель кибератаки?

- Вывести из строя доступность WEB ресурса или IPv4 адреса
- Кража данных. Например, снятие копии дампа СУБД, где хранится информация об пользователях
- Испортить репутацию. Например, подмена текста на главной WEB странице сайта

МегаФон

Какими инструментами можно защитить свои активы?

Сетевая безопасность

- Защита от DDoS
- WAF
- Криптозащита (ГОСТ VPN)
- Интернет под контролем (ИПК)
- Программно-аппаратный комплекс «Информационный периметр» (ПАК ИП)

Консалтинговые услуги и антифрод

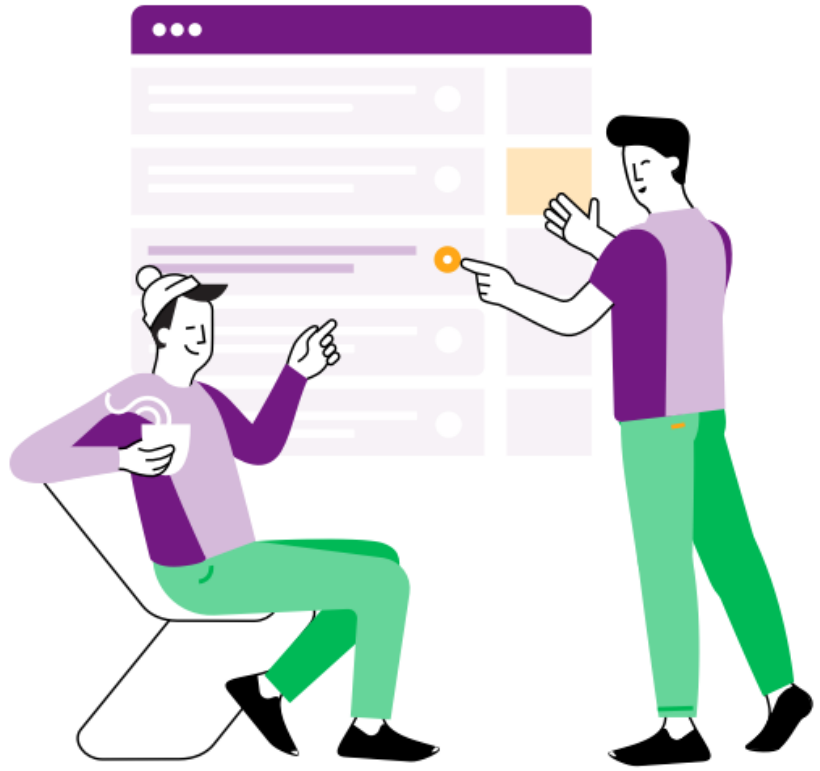
- Сканирование на уязвимости
- Threat Intelligence
- Анализ защищенности (Pentest)
- Антифрод
- Security Awareness

Защита данных

- Защита баз данных
- Защита корпоративной почты
- МегаФон EDR
- МегаФон MDM
- МегаФон DLP

МегаФон

Кейс.
Услуги КБ от МегаФона как инструментарий защиты активов Заказчика



МегаФон

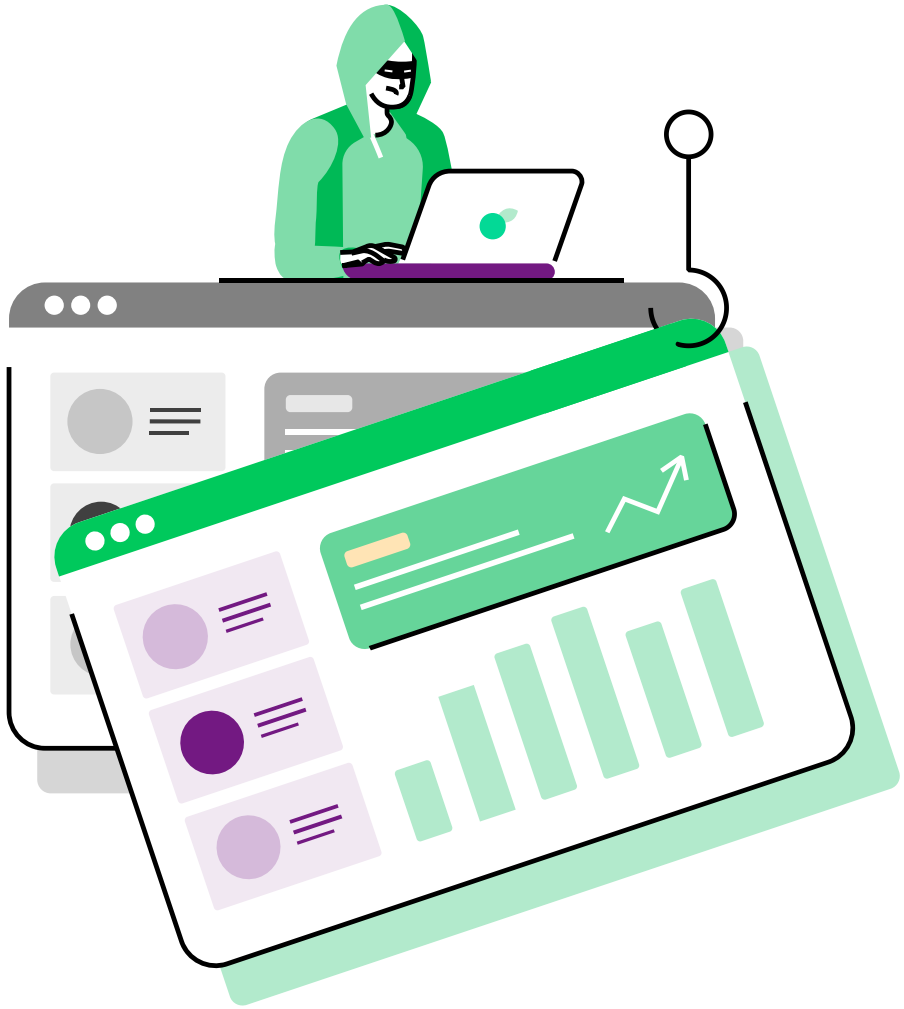
Пример компании, которую мы защитили

Цель проекта:

- Выявить у клиента «проблемные» места в ИТ инфраструктуре
- Предложить инструментарий решения проблем
- Комплексно решить задачи
- Запланировать работы на будущее

МегаФон

Этап 1. Консалтинг



Анализ инфраструктуры по явным возможным уязвимостям

Применили услуги:

«Сканер уязвимостей» и **«PENTEST»**

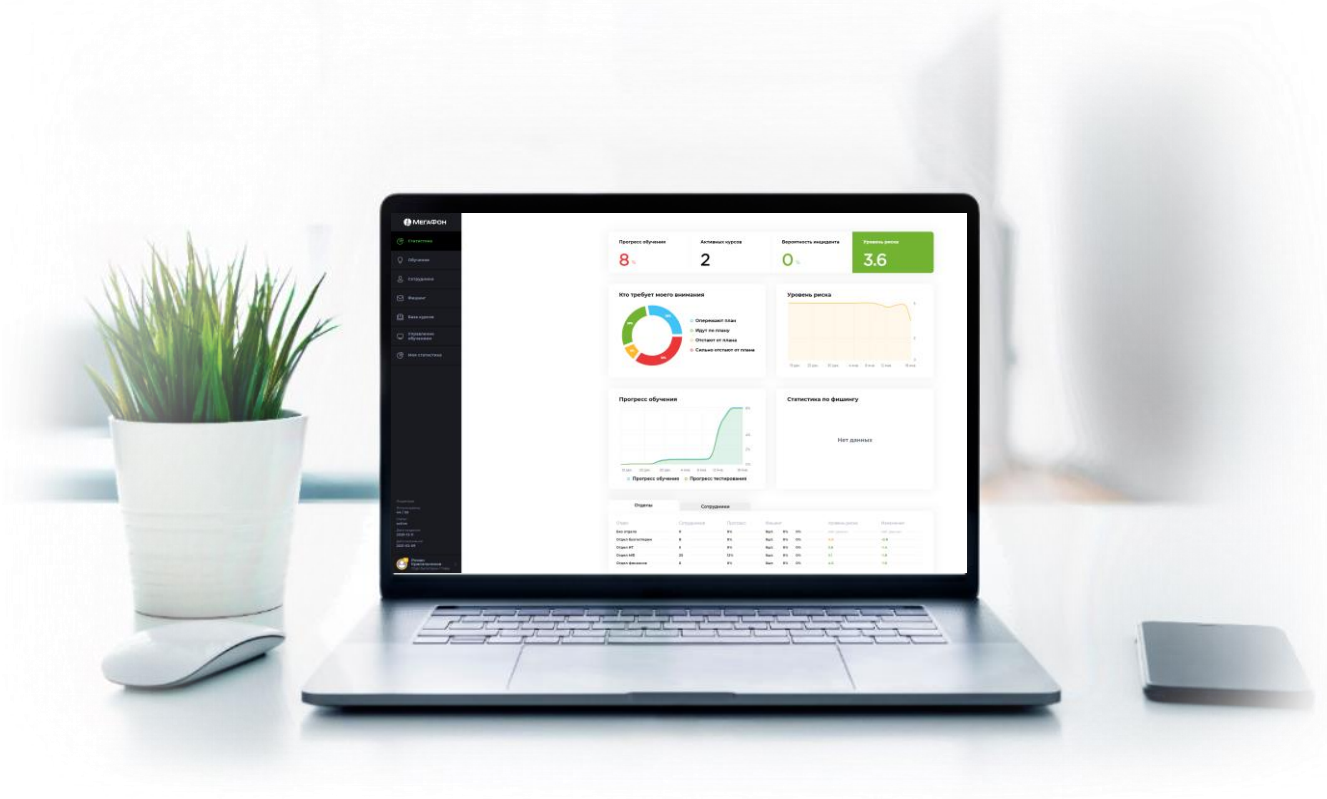
Сформировали отчет в котором отразили:

- Наличие используемого ПО в периметре Заказчика
- Версии ПО и наличие требуемого обновления, чтобы учесть актуальные сигнатуры
- Изучили сетевую топологию
- Составили основную модель угроз и перечень возможных «нарушителей»
- Проверили выполнение регламентирующих правил (нормативы) на наличие средств применения и оформления документации

МегаФон

Этап 2. Выводы

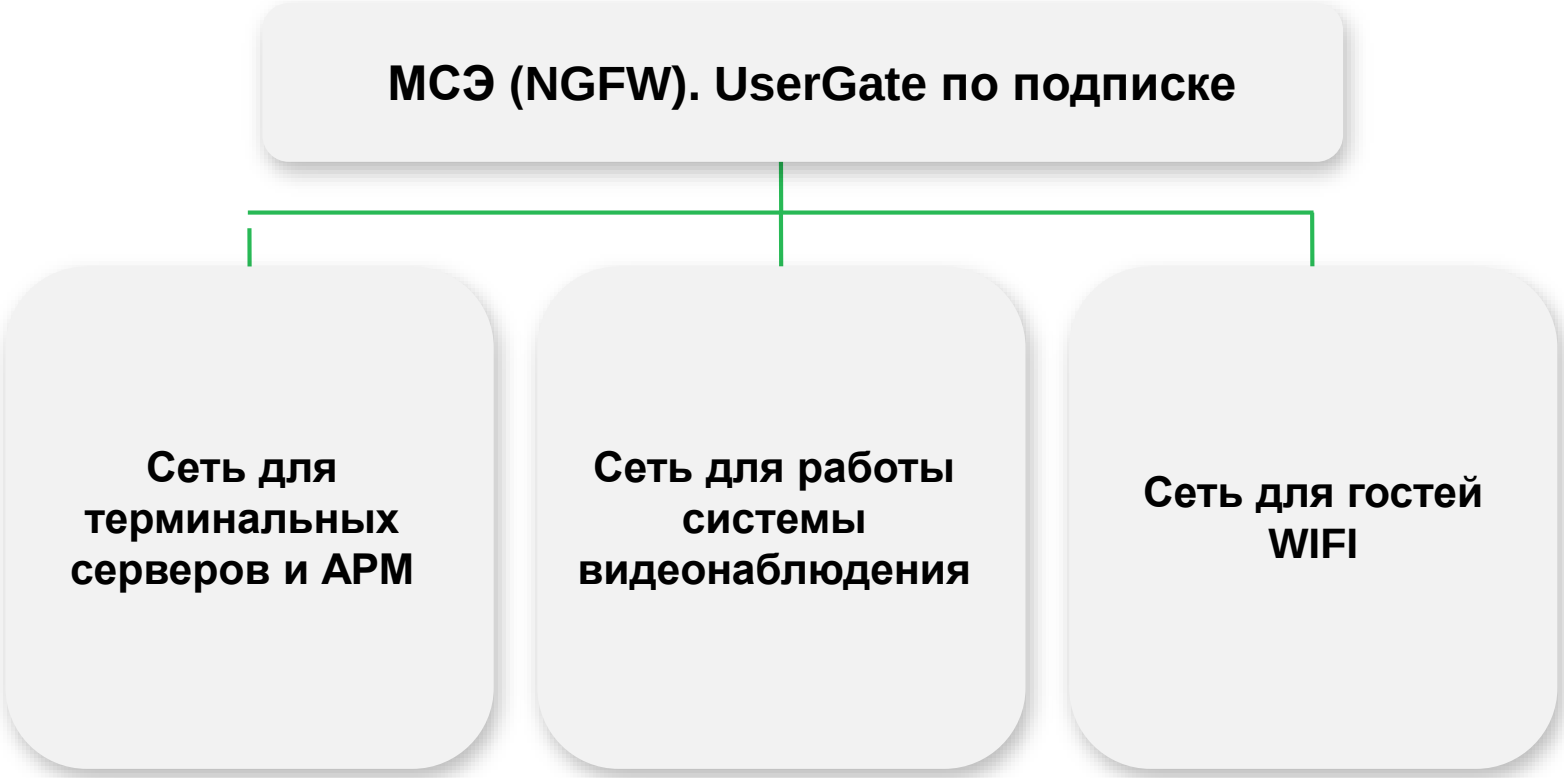
- Заказчик использует ПО, которое не обновлялось уже давно
- Не было разграничения прав у ИТ Администраторов
- Не выполнялись требования нормативной функции или ПО было снято с поддержки от вендора
- Отсутствие разделение сетей, т.е. не было даже DMZ для гостевого WIFI
- Использование сервера терминальных подключение от MS



МегаФон

Этап 3. Решение и реализация средств КБ

Разделили сети заказчика на группы и установили новое ПО



Выводы:

- Заменили текущий МСЭ на UserGate, т.к. вендор оборудования не может оказывать услуги
- Новое ПО МСЭ предоставили в аренду, чтобы можно было оперативно наращивать ресурсы и модули ИБ
- Разделили сети, чтобы минимизировать ущерб злоумышленника при попадании его в корп.сеть

МегаФон

Этап 3. Решение и реализация средств КБ

Убрали сервера терминальных подключение и заменили на решение VDI

Что получила компания перейдя на VDI для ИТ:

- Централизация и унификация рабочих мест
- Управление/изменение АРМ, только через специалиста ИТ
- Снижение требования к офисным ИТ специалистам
- Отсутствие географической привязки к АРМ и его обслуживания
- Резервирование данных. АРМ пользователя, легко зарезервировать, обеспечить бекап данных
- Гарантированная производительность и выделенные ресурсы под каждого пользователя

Выгода для реализации задач от ИБ:

- Обмен данными, только на уровне приложений. Защита от эксплоита RDS. Пример, CVE-2019-0708 (BlueKeep), связан с работой Remote Desktop Services (RDS) и RDP. Перехват прав администратора
- Полный контроль за действиями конкретного пользователя
- Установка доп.ПО, например, DLP
- Всегда известно, какой пользователь, что делает и быстро определяется возможная точка взлома
- Антивирус не отъедает ресурсов самого АРМ

МегаФон

Этап 3. Решение и реализация средств КБ

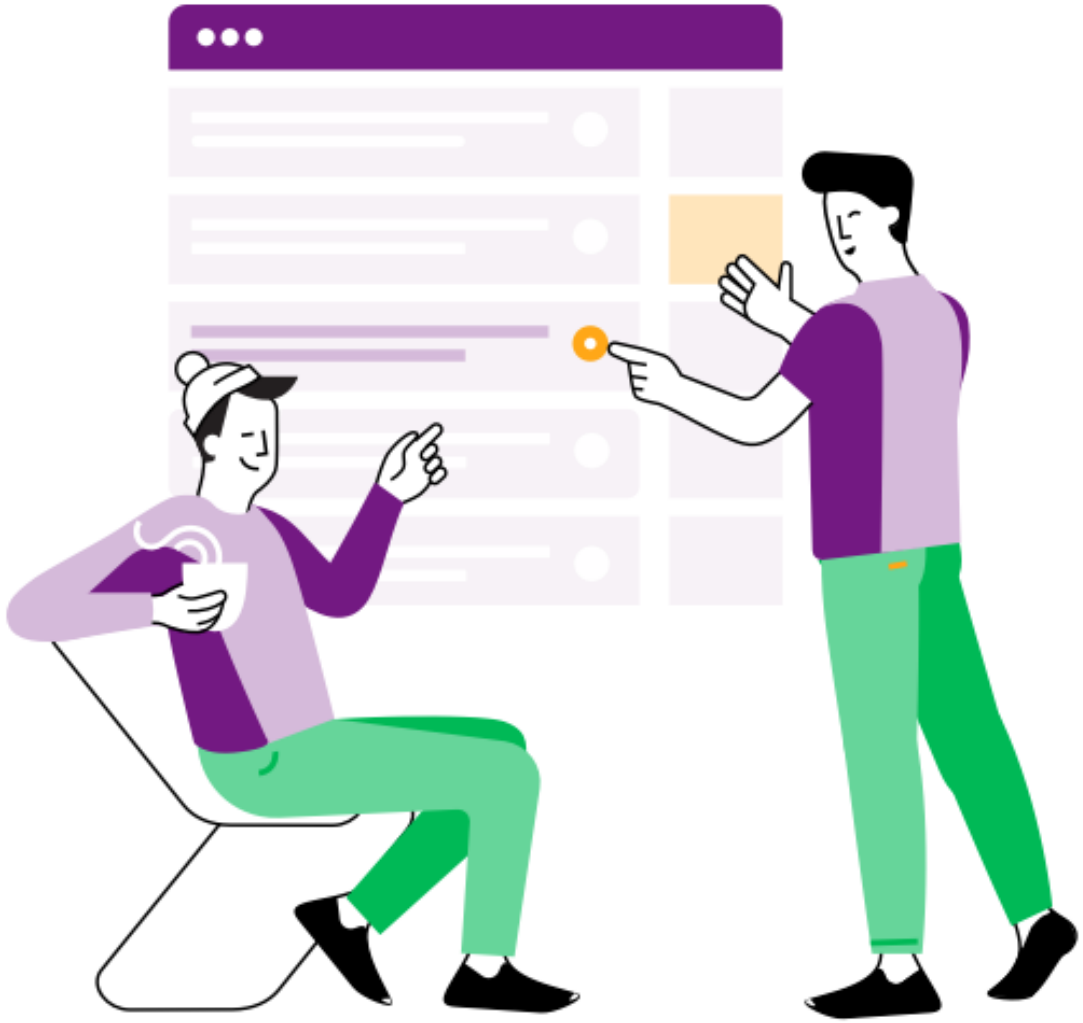
Запланировали работы на будущее

- Установить систему Защиты Базы Данных (ЗБД), чтобы логировать все доступы события, связанные с СУБД, в том числе и действия администраторов
- Завершить пилот DLP, т.к. внедрение VDI завершено
- Провести обучение для персонала. Внедрение решения Security Awareness (SA). Портал обучения и тестирования персонала в вопросах ИБ и проведение учебных фишинговых атак

МегаФон

Выводы из кейса

- Внедрили логирование всех событий ИТ и ИБ, что помогло оптимизировать работу специалистов Заказчика
- Применяемые ранее средства ИБ не работают в настоящем времени
- Обновление и поддержка от вендора важная составляющая в любой ИТ инфраструктуре
- Социальный хакинг важный фактор ИБ, который нужно учесть



МегаФон

Бонус!

Чек лист действий:

- Описать свою сетевую ИТ Архитектуру
- Составить список текущего системного ПО с описанием версий и наличия обновлений
- Запустить «Сканер Уязвимостей» в локальной сети, чтобы получить автоматизированный отчёт об открытых портах, наличия не учтённого ПО и прочее
- Выделить отдельного специалиста для решения инцидентов ИБ
- Продумать и внедрить ПО, которое сможет выявлять инциденты. Минимум это DLP и СОВ (NGFW), в идеале SIEM.
- Периодически проводить PenTest для выявления узких мест в ИБ и получения рекомендаций
- Обязательно учить персонал грамоте в вопросах ИБ и проводить учения

Технологии включают бизнес

Погоржельский Станислав
Руководитель по технологической поддержке облачных и инфраструктурных решений

stanislav.pogorzhels@Megafon.ru

8 800 550 05 55
b2b.megafon.ru

МегаФон | ПроБизнес