Как построить безопасную удаленку без незваных гостей?

BELYAEV

Спикер: Беляев Д.А

Боль

Ошибка

1. Неверная настройка программного обеспечения (conf+Cloud);
2. Нехватка компетенций (sec+staff);
3. Работа из под открытых Wi-Fi сетей.

Фатальная ошибка

1. Слабая защита каналов связи;
2. Отсутствие мониторинга;
3. Отсутствие плана реагирования;
4. Отсутствие обновлений;
5. Отсутствие защиты от ВПО;
6. Отсутствие контроля доступа;
7. Отсутствие резервного копирования;
8. Отсутствие защиты физического доступа к устройству;
9. Отсутствие шифрования.
10. Не правильно построенная архитектура удаленного доступа.

Аналитика

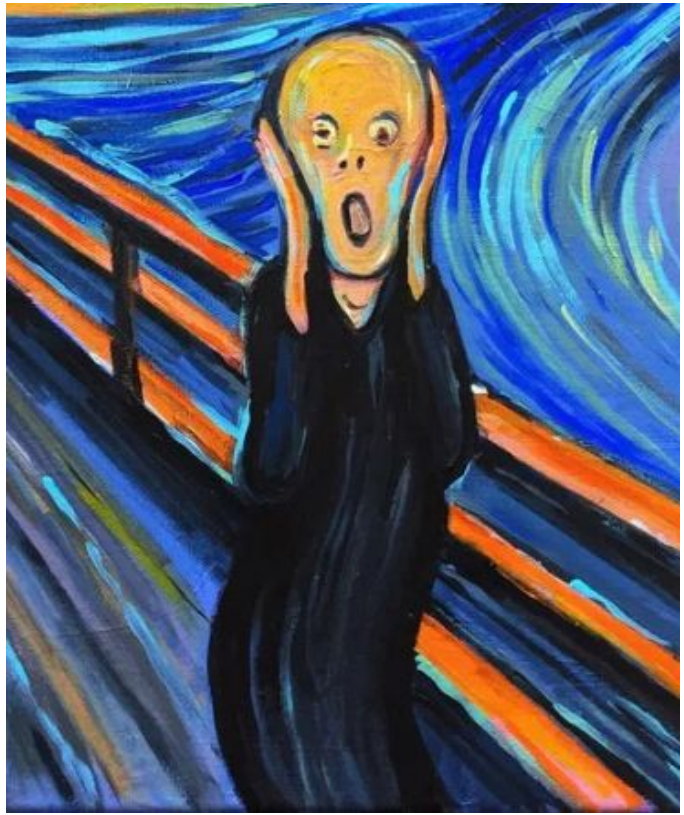
1. SolarWinds: В декабре 2020 года было обнаружено, что хакеры взломали SolarWinds, компанию-разработчика программного обеспечения для мониторинга сетей, и внедрили зловредное ПО в их продукты. Одним из методов, использованных при этом, был доступ к внутренней сети компании через учетные данные сотрудника.

2. Target: В 2013 году хакеры взломали системы Target, крупнейшей розничной сети в США. Они использовали учетные данные контрактного сотрудника компании, который имел удаленный доступ к системам компании.

3. Home Depot: В 2014 году хакеры взломали системы Home Depot, крупнейшей сети магазинов товаров для дома в США. Они использовали учетные данные контрактного сотрудника компании, который имел удаленный доступ к системе.

4. RSA: В 2011 году хакеры взломали системы RSA, компании, производящей аутентификационные токены для входа в системы безопасности. Они использовали учетные данные сотрудника компании для доступа к системе.

5. Anthem: В 2015 году хакеры взломали системы Anthem, одной из крупнейших страховых компаний в США. Они использовали учетные данные сотрудника компании для доступа к системе.



Решение проблемы

1. Провести аудит в компании;
2. Разработать регламент по безопасности удаленного доступа;
3. Издать приказ;
4. Провести работу над ошибками;
5. Осуществлять контроль.

1. Закупка/настройка МСЭ/ NGFW;
2. Осуществлять обновления ОС и ПО;
3. Реализовать защиту от ВПО;
4. Реализовать контроль доступа;
5. Реализовать контроль каналов утечки;
6. Реализация резервного копирования;
7. Реализовать защиту физического доступа к устройству;
8. Настроить шифрование;
9. Аудит и разработка архитектуры;
10. Проверка настроек ПО (conf+Cloud);
11. Обучение (sec+staff);
12. Шифрование Wi-Fi каналов;
13. Разработать план реагирования;
14. Осуществлять мониторинг.

Виды удаленки:

Примитивный

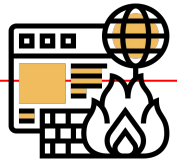
- AnyDesk;
- AMMYY Admin;
- TeamViewer;
- VNC;
- и их аналоги.

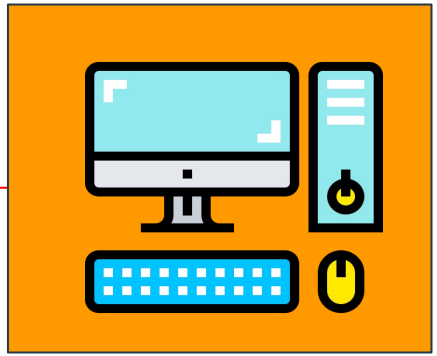
Причины:

- Отсутствует бюджет;
- Отсутствуют компетенции;
- Нехватка времени/штата;
- Пришел на руины.

Схема работы

AnyDesk





Виды удаленки:

“Студент”

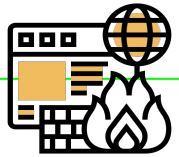
OpenVPN

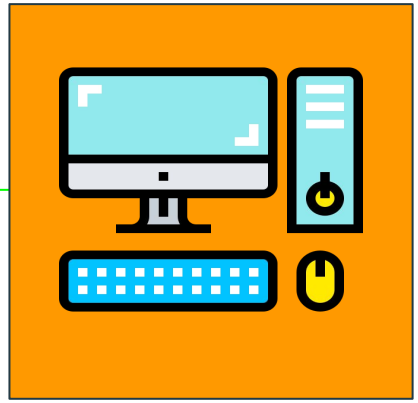
Причины:

- Отсутствует бюджет;
- Имеются базовые компетенции;
- Так исторически сложилось;
- Пришел на руины.

Схема работы

OpenVPN
+RDP





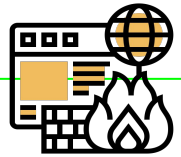
Виды удаленки:

“Специалист”

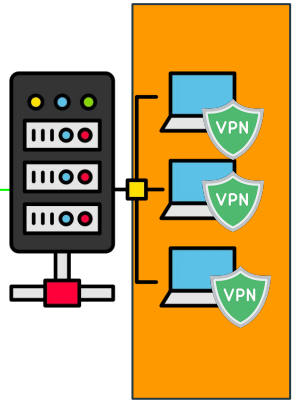
Подключение через сертифицированный VPN/МСЭ с IPSec

Схема работы

Sert VPN+
RDP



NGFW

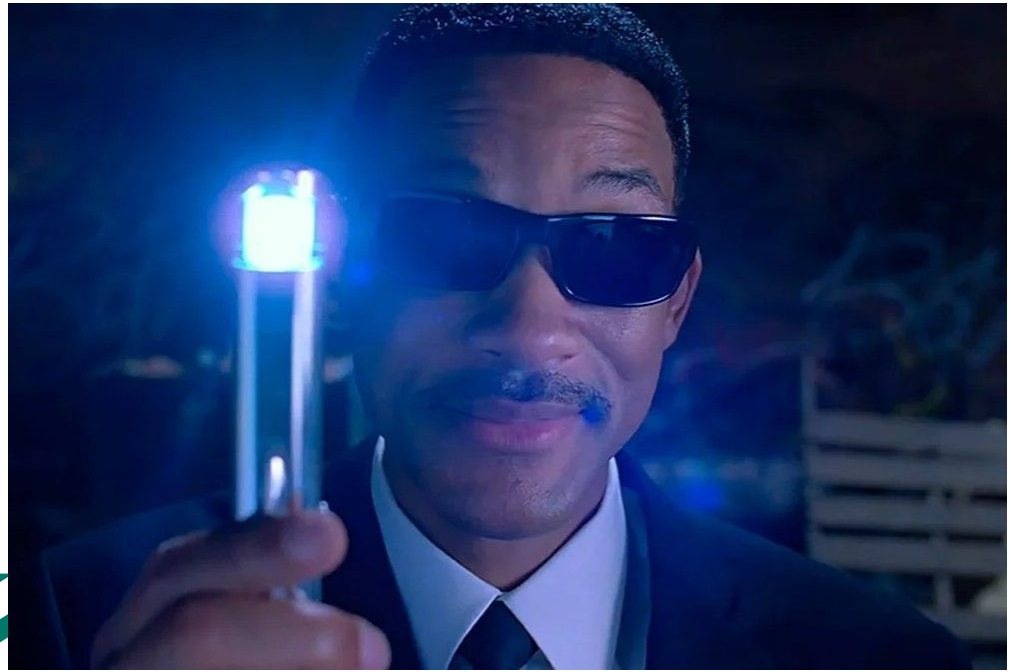


Время менять подходы

«Улучшать — значит меняться, поэтому быть совершенным — значит меняться часто»

Уинстон Черчилль

Спасибо за внимание!



Ваши вопросы?

da.belyaev

@da_belyaev

+7-905-486-49-11

da.belyaev@mail.ru

Беляев Дмитрий Александрович
Начальник СИБ

АО ПЕРВЫЙ ИНВЕСТИЦИОННЫЙ БАНК