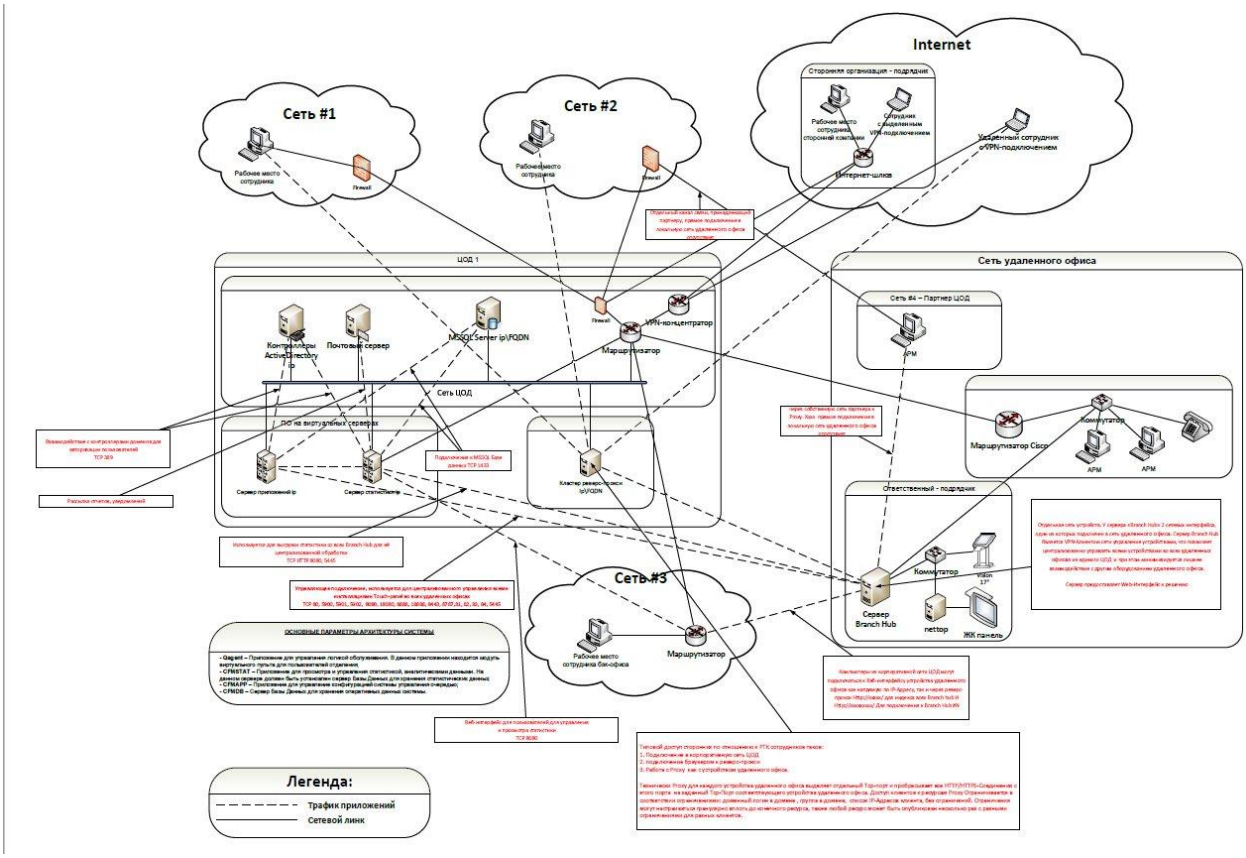
Домашка № 3

Лешков И.А.

Задание №1.

К уроку приложена схема реализации цифрового проекта. Составить свое экспертное мнение по поводу защищенности планируемой реализации, IT-инфраструктуры и ландшафта, составить предложения по модернизации схемы и внедрению средств защиты (процессы защиты) в.т.ч. и исходя из материалов текущего урока.



Глядя на ИС выше, можем выделить следующие сегменты:

1. ЦОД (центр обработки данных) со своей сетью.
2. 3 корпоративных сети, каждая из которых имеет доступ к данным ЦОД.
3. Зона internet, где с ЦОД взаимодействуют организация-подрядчик и сотрудник с удалённым доступом.
4. Сеть удалённого офиса, где у нас располагается 3 подсети: партнёр-ЦОД и ответственный подрядчик, который может управлять всеми устройствами во всех удалённых офисах из единого ЦОД.

Буду идти по порядку, останавливаясь на моментах, на которые стоит обратить внимание:

- ✓ Сеть #3 нужно расположить за WAFом.
- ✓ Фаерволл ЦОД охватывает не весь периметр ЦОД (как мне кажется, он некорректно настроен для входа из сегмента internet – это плохо.) Видим, что подрядчик и удалённый

сотрудник через VPN-концентратор и маршрутизатор могут достучаться до ПО на виртуальных серверах.

- ✓ Использован стандартный уязвимые порты для подключения к MSSQL БД >>> 1433
- ✓ Взаимодействие с контроллерами доменов для авторизации пользователей через LDAP на стандартном незащищенном порту тсп/389 (используем SLL LDAP на 636-м порту).
- ✓ Порты открытые для выгрузки статистики оставляют вопросы...(tcp/5445 порт – блок сообщений сервера через удаленный прямой доступ к памяти, зачем он тут?), ну и http (выгрузка данных по незащищенному протоколу, которые могут содержать конфиденциальную информацию).
- ✓ Управляющее подключение между сервером приложений и сервером brunch Hub – открыто слишком много портов (нужно проанализировать/протестировать их и оставить необходимые и защищенные).
- ✓ Опять же, видим веб-интерфейс для пользователей сетки 3, которые могут просматривать и управлять статистикой через незащищенное соединение.
- ✓ Компьютеры из корпоративной сети ЦОД могут подключаться к Вэб-интерфейсу устройства удаленного офиса как напрямую по IP-Адресу, так и через реверс-прокси Http://xxxxx/ для индекса всех Branch hub и Http://xxxxxxxxx/ Для подключения к Branch Hub #N. Может здесь стоит оставить подключение через реверс-прокси и по https?
- ✓ И ещё момент, соединение удалённого офиса с сервером Brunch Hub через коммутатор, мне кажется, не лучшая идея… Думаю, соединиться лучше через маршрутизатор Cisco (опять же, наличие фаерволла на границах было бы неплохо).

Резюмируя всё и опираясь на опыт “best practice”, для данной конфигурации неплохо было бы использовать:

- Чёткое разграничивание сетей с настройкой фаерволлов на границах.
- Может быть даже избавление от лишних сегментов сети, таких как концентратор VPN (поднять вместо этого данный сервис на WAF)
- Возможно, сеть ЦОД слишком перенасыщена и можно было бы её поделить на сегменты с отдельной адресацией на каждый сегмент.

Очевидно, что внутри данной конфигурации есть достаточное количество чувствительной информации (те же базы MySQL, ActiveDirectory и.т.д.) и утечка этих данных ничего хорошего не сулит. А посему, важно:

- Проверить сети и узлы на наличие уязвимостей, провести пентест.
- Произвести установку антивирусного ПО на всех серверах и рабочих машинах

- Также, неплохо было бы внедрить систему обнаружения вторжений для отлавливания и логирования действий потенциальных злоумышленников.
- На особо важных узлах, где сотрудники имеют доступ к особо чувствительной информации – провести ликбезы по парольной, веб-безопасности и.т.д.

//Done… ☺