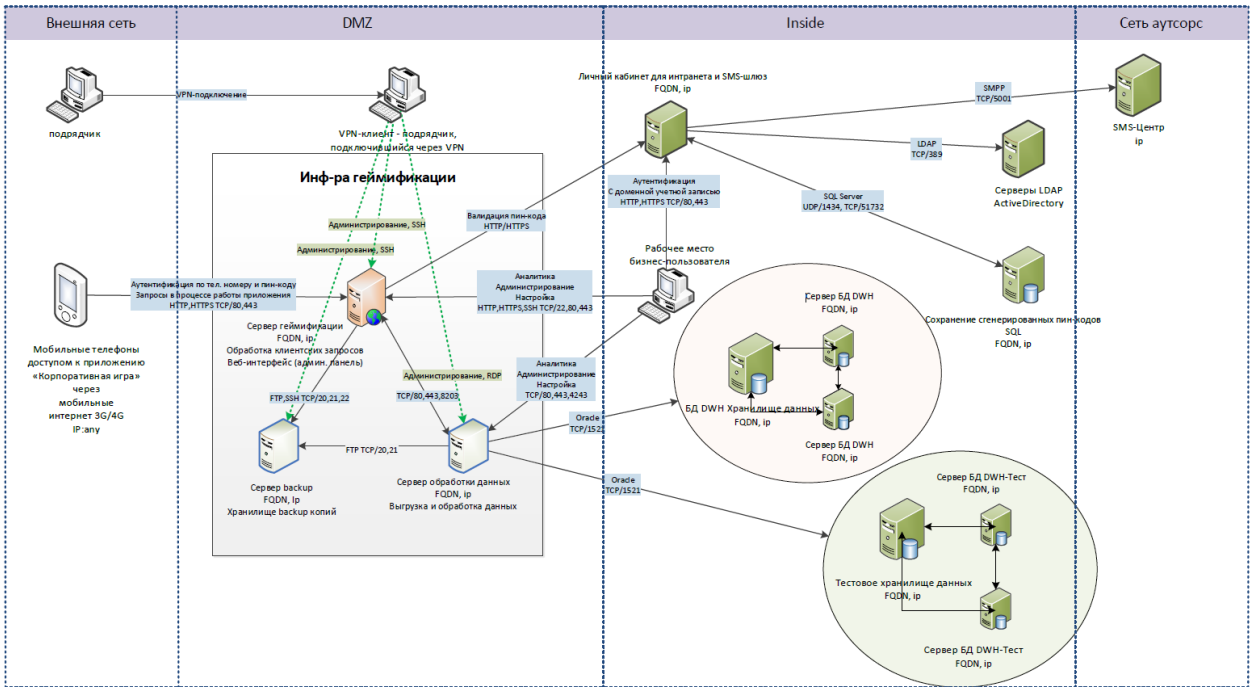
Домашка № 2

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 4 сегмента:

1. Внешка (интернет >>> пользователи мобильных устройств, подрядчик)
2. Демилитаризованная зона (здесь у нас есть фирма-подрядчик, которая через VPN производит администрирование серверов зоны через SSH, а также через удаленный доступ к рабочему столу RDP)
3. Зона inside (частная сеть интранета, где реализованы: личный кабинет + смс-шлюз, службы каталогов ActiveDirectory через LDAP, SQL сервер, а также два хранилища данных (тестовое и рабочее) в связке с серверами БД, куда выгружаются данные из DMZ, а также рабочее место бизнес-пользователя)
4. Сеть аутсорс (с sms-центром на борту).

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

- ✓ Запросы к серверу геймификации по HTTP – я бы убрал.
- ✓ Сообщение между серверами в зоне DMZ через незащищённый ftp-протокол, тоже не лучшая идея (трафик можно прослушать).
- ✓ Да, и ещё аутентификация по телефонному номеру/пин-код через смс, не то чтобы очень надёжный способ, потому как

пин-коды обычно достаточно маленькой длинны и легко подвергаются брутфорсу + злоумышленник может перехватить пин и аутентифицироваться вместо легитимного юзера.

- ✓ Валидацию пина по HTTP тоже стоит убрать.
- ✓ Подрядчик должен иметь ограниченный уровень доступа к информации на серверах, достаточный для администрирования.
- ✓ Я бы закрыл порт 8203 между сервером геймификации и сервером обработки данных, не совсем понимаю зачем он тут нужен и в доступе по SSH от сервера геймификации на backup-сервер, мне кажется, тоже нет необходимости.
- ✓ Видим, что данные с сервера обработки данных выгружается в инсайд БД-х (вендор – Oracle) по стандартному 1521 порту, может быть лучше переключить на порт 2484 для более защищенного подключения.

Далее идём в инсайд:

- ✓ Мне не совсем понятен, кто здесь является бизнес-пользователь? Но, что-то подсказывает, что прав на чтение + аналитика может быть тут было и достаточно и убираем уязвимые порты и протоколы (80 и Http), в том числе и для аутентификации в личном кабинете (не знаю насколько хороша идея аутентификации с доменной учетной записью?).
- ✓ Так или иначе, сервер где располагается личный кабинет связывается с очень чувствительными узлами, такими как - сервер Active Directory (служит единым хранилищем данных для быстрого доступа к данным для всех пользователей и контролирует доступ для пользователей на основе политики безопасности каталога) по протоколу LDAP, а также SQL Server где хранятся сгенерированные пины. Поэтому данный узел должен быть надёжно защищен от компрометаций.
- ✓ Соединение с Active Directory лучше бы осуществлять по 636 порту tcp, а из подключения к SQL-серверу, наверное, можно убрать стандартный порт udp/1434.

Что касается сегмента «аутсорс»:

- ✓ Здесь достаточно однозначная связь, сервер посылает короткие сообщения через SMPP порт 5001 в смс-центр, тот в свою очередь шлёт смс с пин-кодом пользователю на мобильное устройство. Что здесь может пойти не так, мне сложно сказать...

И в заключение, хотелось бы отметить то, что данная ИС содержит в себе персональные данные, которые, скорее всего попадают под 1 или 2 уровень защищенности, согласно постановлению Правительства РФ от 1 ноября 2012 г. N 1119 "Об утверждении требований к защите персональных данных при обработке в информационных системах персональных данных", и Приказу ФСТЭК №21 от 18.02.2013г., и поэтому защита этих данных должна осуществляться в соответствии с требованиями вышеперечисленных регуляторных документов, а также сюда относятся и будут иметь применимость 149-ФЗ «Об информации, информационных технологиях и о защите информации», 152-ФЗ «О персональных данных».

Согласно этим документам, есть базовый набор средств защиты по отношению к каждому конкретному уровню защищенности (внедрение антивирусной защиты, установка и настройка систем обнаружения вторжений, наделение доступом субъектов доступа к объектам доступа, контроль и анализ защищенности ПДн, и.т.д).

//Done… ☺