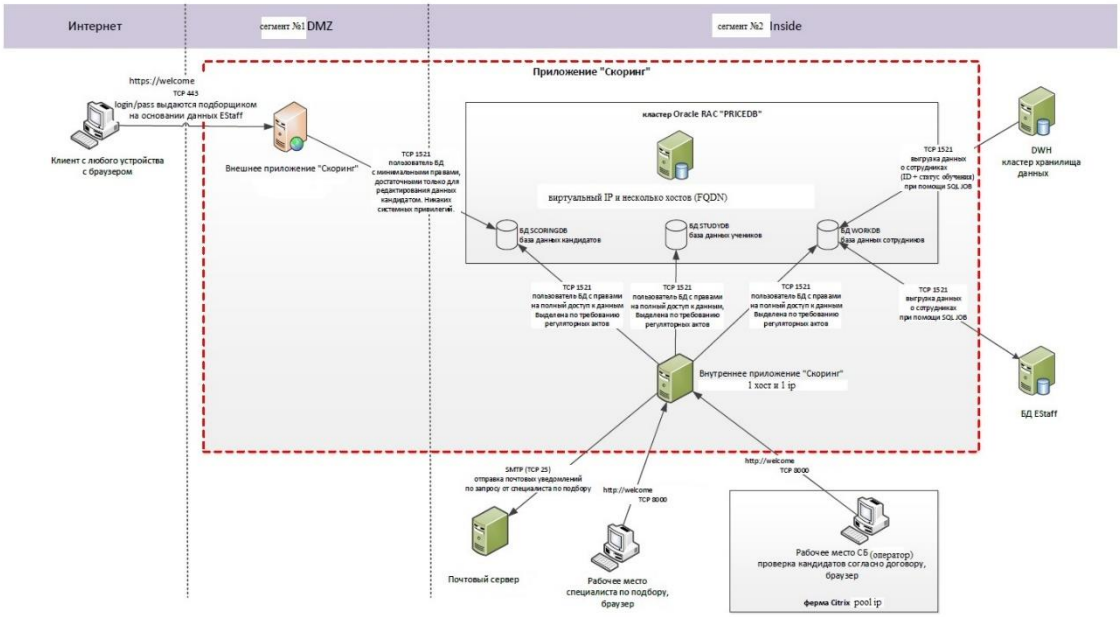
Домашка № 4

Лешков И.А.

Задание №1.

К уроку приложена схема реализации цифрового проекта. Составить свое экспертное мнение по поводу технической защищенности планируемой реализации, IT-инфраструктуры и ландшафта. Предложить возможные варианты эксплуатации и настроек рассмотренных инструментов в уроке применительно к приложенной схеме реализации цифрового проекта.



Изучая предложенную реализацию «Скоринга» и it-инфраструктуры, хотелось бы отметить наличие демилитаризованной зоны, как дополнительной ступени защиты локальной зоны от внешних атак (у злоумышленника есть прямой доступ лишь к приложению в этом сегменте). Это хорошо. Однако, есть ряд моментов на которые стоит обратить внимание:

- Необходимо внедрить дополнительную ступень защиты в виде FW на границе с внутренним сегментом, возможно, поднять сервис VPN на нём же, где принимать клиентов и далее уже через FW пропускать трафик в инсайд.
- Также, в данной зоне можно задуматься и о внедрении сервера управления антивирусными решениями, который будет агрегировать и коррелировать события со всех устройств (через дополнительный фаерволл), на которых нужно будет установить антивирусное ПО (будь то, обычные рабочие станции сотрудников, либо же сервера с чувствительной информацией)
- Что касается инсайда, то, как я и упомянул выше, используя опыт «бэст практисов», необходимо строго разграничить доступ к информации для каждого отдельного клиента, установить средства защиты в виде антивирусного ПО (например, почтовый антивирус, так как имеем почтовый сервер).

- Вероятно, доступ к внутреннему приложению «Скоринг» нужно осуществить через WAF, в котором «по белому списку» настроить доступ сотрудников, кто имеет полный доступ к базам данных, а кто только ограниченный функционал.
- Внедрение DLP-систем не будет лишним.
- Также, обязательным решением, я бы внедрил пентест и тестирование всех защищенных узлов при помощи специальных сканеров (стоит уделить внимание сканированию на возможности компрометаций БД, возможности проведения инъекций в них, и.т.д) и при обнаружении дыр – рекомендации по патчингу. Контроль актуальных версий, как вытекающая необходимость.
- Стоит также разграничить пользовательский сегменты сети и серверные сегменты.
- Можно настроить SIEM-систему и проверить подключение целевых узлов к данной системе.
- Настроить упорядоченное логирование событий.
- Ну и конечно же, стоит задуматься об отдельном сервере для размещения бэкапов и возможности быстрой реанимации системы, в случае непредвиденных форс-мажорных обстоятельств.

//Done… ☺