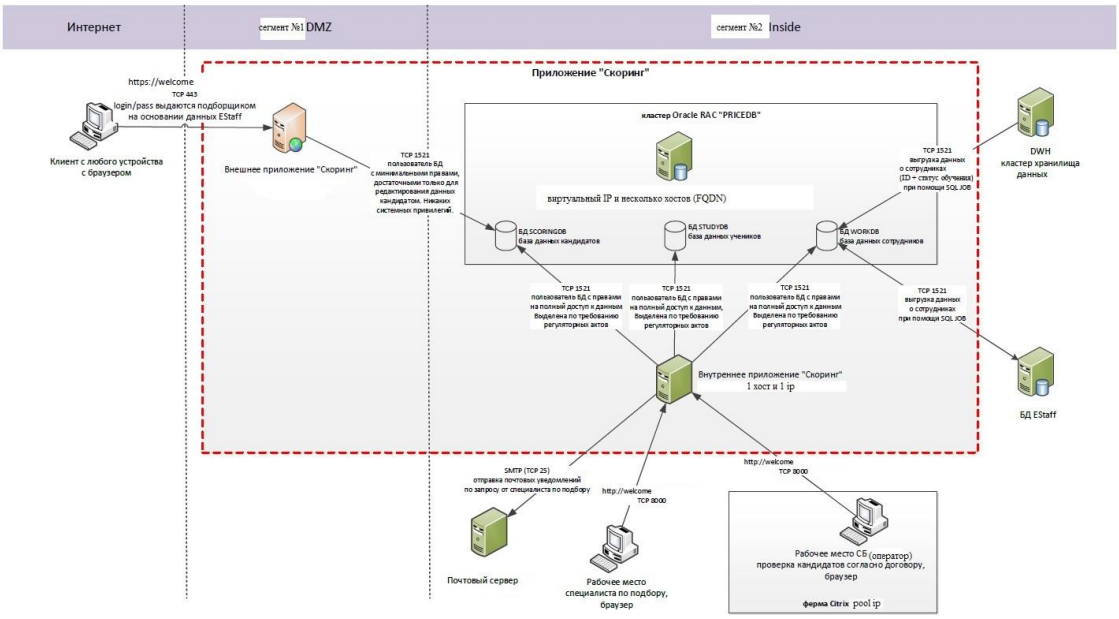
Домашка № 1

Лешков И.А.

Задание №3.

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).



«Скоринг» – используемая банками система оценки клиентов, в основе которой заложены статистические методы.

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:

- Внешнее приложение выдаёт комбинации логин/пароль на основании данных из базы Estaff. А в данной базе содержаться учётные данные сотрудников. Соответственно по выданные комбинации, по сути, могут дать информацию потенциальному злоумышленнику о длине пароля/логина, их формате и.т.д, что в свою очередь может позволить выявить определённые закономерности в комбинациях(к примеру, если зарегистрироваться с разных аккаунтов и получить несколько пар login/pass) и попытаться подобрать легитимные данные одного из сотрудников. Поэтому, наверное – это не лучший способ предоставления учетных данных. Разве что, в них не должно быть никаких закономерностей. Так или иначе все пароли должны быть надёжно захешированны с использованием криптостойких алгоритмов шифрования.

- Далее видим, что данные о кандидатах улетают во внутренний сегмент >>> БД кандидатов. И видно, что пользователь БД наделён хоть и минимальными правами без системных привилегий, однако редактировать данные можно. При работе с БД важно валидировать вводимые данные от клиентов из вне, но не только на входе, но и на границах компонентов систем (в каждом запросе) во избежание инъекций в БД или использовать параметризованные запросы.

- По поводу кластеризации мне сложно сказать, я не совсем компетентен в этом вопросе. Но рискну предположить, что нахождение БД кандидатов, с которой у нас контачит внешнее приложение, в одном кластере с другими базами – не есть хорошо. Но, могу и ошибаться)

- Почтовый сервер настроен на получение сообщений от приложения по стандартному SMTP-протоколу на 25 порту. Это не лучшее решение, так как предаваемая информация никак не шифруется. Поэтому для данного почтового сервера лучше использовать соединение на 465 порту (SMTPS) или использовать команду-расширение “STARTTLS” для создания шифрованного соединения.

- Что касается рабочего места специалиста по подбору и рабочих мест операторов по проверке кандидатов (ферма Citrix), то данные клиенты связываются с внутрянкой по протоколу “HTTP” на 8000 tcp порту, соответственно, имеем нешифрованный трафик. Видим, что у внутреннего пользователя БД приложения есть полный доступ ко всем базам данных. Исходя из того, что специалист по подбору и операторы по сути работают с конфиденциальными данными, обращение к данному хосту стоит осуществлять через шифрованное соединение (например на 443 порту tcp).

- Ну и напоследок >>> WAF! (между интернетом и DMZ). Может он просто не отображён на схеме, но поднастроить не мешало бы (чёрные или белые списки последовательностей символов, экранирование текста запроса, и.т.д).

//Done… ☺