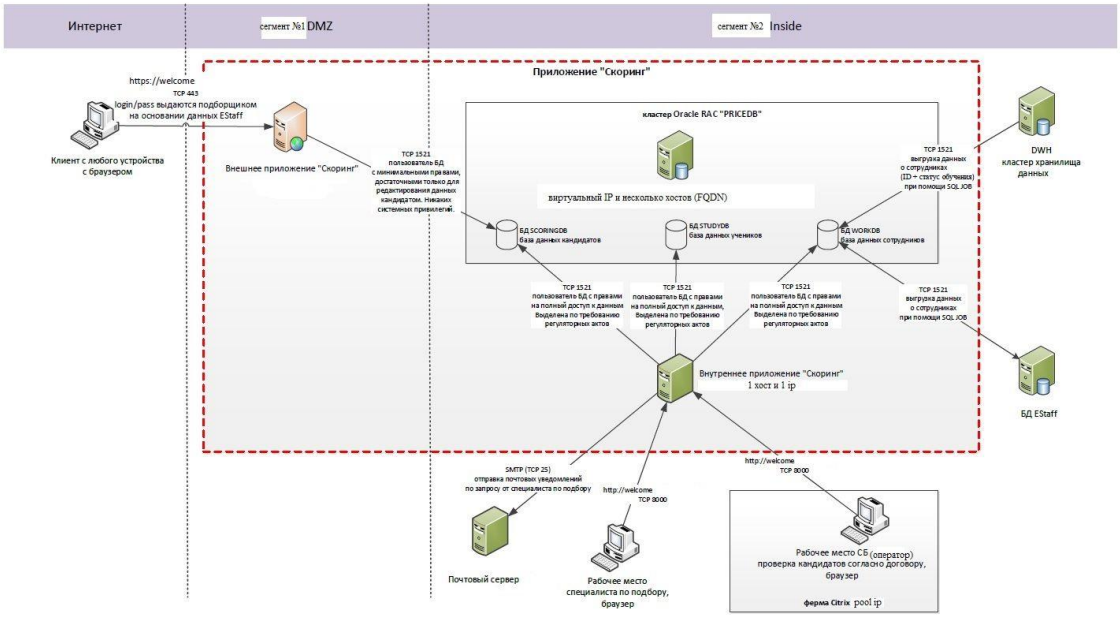
Хананиев Даниил Владимирович
Курс «Подготовка к собеседованию специалиста по информационной безопасности», поток от 20.05.2020
ДЗ № 4



1. Сразу отмечу, что и внутри защищенного периметра нужно использовать https, а не http.

2. Антивирус на каждом рабочем месте и серверах. На входе внутрь периметра, кроме файрвола должен стоять антивирус, причем другого вендора, чем на клиентах. На серверах тоже вендор отличный от производителя антивируса на рабочих местах. Так мы обеспечим необходимое перекрытие.

3. Антиспам на клиентские машины.

4. Так как мы имеем дело с чувствительными данными, необходимо внедрять систему DLP.

5. На серверах внешнего и внутреннего приложения нужно поставить WAF, это сервера активно работают с БД, потому нужно обеспечить безопасность передаваемых данных от всякого рода иньекций, плюс мониторинг нестандартной работы пользователей. Функция защиты БД тут пригодится. Принцип AAA тоже диктует нам необходимость контроля над аутентификацией и авторизацией.

6. Также сервера приложений регулярно должны проверяться сканерами безопасности, и код, и обновления приложений, должны тестироваться на секьюрность.

7. Третье А – аудит. Все вышеперечисленное, а особо инциденты, должно обязательно логироваться, с внятной системой обработки и реакции на инциденты.

Отмечу, что все вышеперечисленное достаточно дорого, потому решение о внедрении того или другого компонента должно приниматься на основании определенной информации, такой, к примеру как: ценности защищаемых данных, требований надзорных органов, финансовой состоятельности компании. Но при этом, есть определенный минимум, который строго должен

быть реализован. Это файрвол, антивирус, антиспам, тестирование кода приложений, логирование, внедрение только безопасных протоколов с безопасной криптографией, контроль пользователей и их прав – следование принципам Least privilege и Need to know, и, в общем, следование принципу AAA.