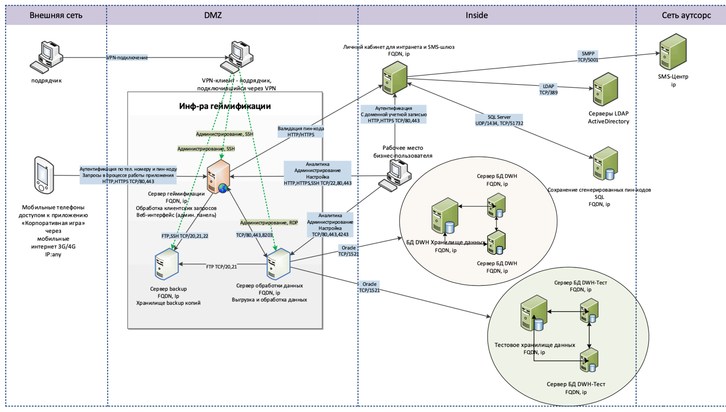
ДЗ №06 - Денис

Урок 6. Информационные системы обеспечения информационной безопасности и средства защиты. (Часть 3)

1. 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 2-6 уроков.

Подготавливается к сдаче к уроку 7.

Практическое задание к схеме 2



Сразу сведем в табличку:

Наименование средства защиты	Цели, прикладное размещение и необходимость использования
Применение СКЗИ	В данном ландшафте наблюдаются небезопасные соединения, а так же работа с пин-кодами, информация в БД - это могут быть персональные данные. Как минимум обернуть трафик в SSL. Обеспечить сохранение сгенерированных пин-кодов в шифрованном виде согласно требованиям ФСБ, это же касается в случае чувствительной информации или персональных данных в БД в случае угона злоумышленником. Рекомендуется внедрить поддержку токенов для мобильного приложения.
Подключение SOC центра	Для повышения защищенности и скорости реагирования, аналитики и комплексного мониторинга рекомендуется подключить SOC. Это же повысит качество оценки рисков ИБ, фокусировка на слабых местах. Прогнозирование рисков. Особенно удобно и эффективно будет внедрение SOC на базе SIEM.
Обеспечение процесса пентестинга	Рекомендуется по возможности регулярные пентесты, как локальные от компании-владельца продукта, так и от независимых экспертов. Атака и защита неразрывно связаны друг с другом. Это позволит поддерживать в тонусе всю инфраструктуру, вовремя выявлять современные текущие угрозы и устранять слабые места.
Использование анализаторов кода	Рекомендовано, если в сети осуществляются какие-то финансовые или иные ценные транзакции, например, какие-то покупки в игре.
Необходимость подключения Anti-fraud	В случае рисков потери ценной информации, денежных махинаций - да. Зависит от того, какая информация, какие транзакции на контуре.

Задание выполнено!

2020.11.17 19:55