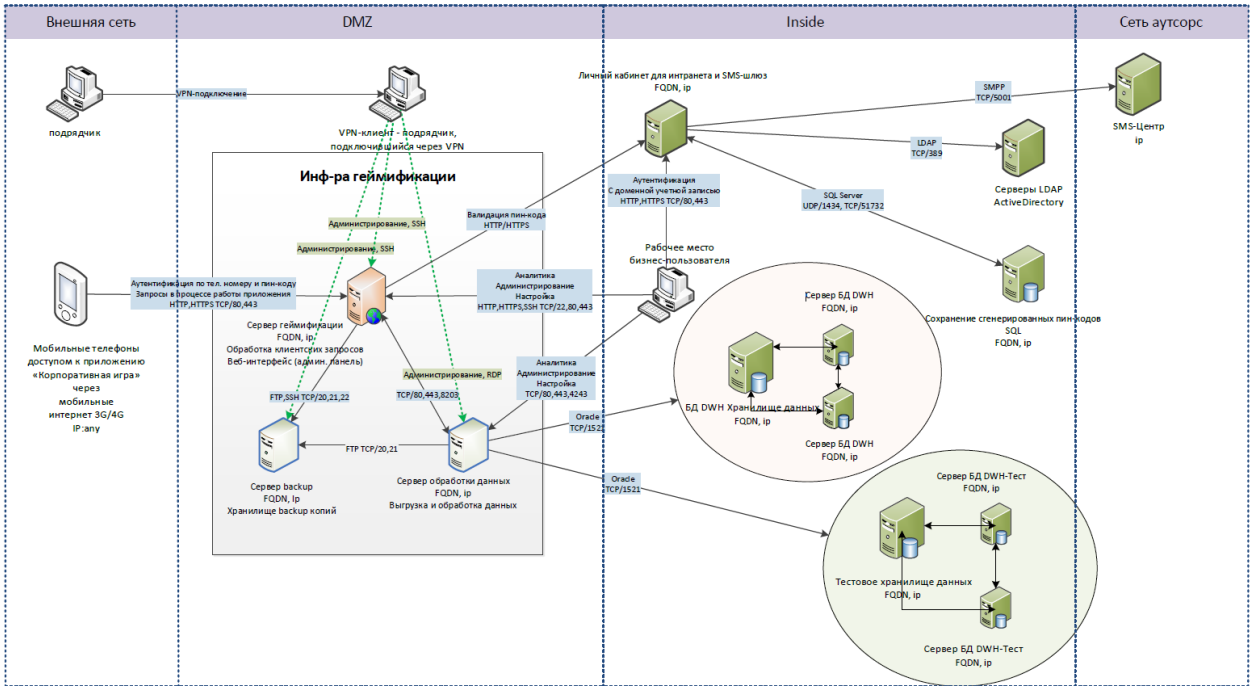
Домашка № 5

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.



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).

Как я уже писал в предыдущем задании по этой схеме, 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, а также, опираясь на современные «бестпрактисы» (стандарты ISO 27K), 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).

Так вот, прибегая к информации, полученной из данного урока, а именно касательно тех СЗИ, которые могут предотвратить вторжения в систему, компрометацию чувствительных данных, их утечку и.т.д, можно предложить следующее:

- На границе с внешней сетью в DMZ внедрить Next-Gen IPS систему, которая могла бы обнаруживать и регистрировать события по НСД в режиме реального времени, а также своевременно использовать функционал для предотвращения атак, прогнозирования возможных уязвимостей и последующих атак на них, определения расположения атакующих и соответствующее документирование угроз.
- Также можно настроить работу SIEM-ситемы между инсайдом и DMZ, которая будет осуществлять сбор и обработку информации о состоянии ИБ со всех узлов защиты (фаерволлы, длп-системы, антивирусное ПО на рабочих станциях, события в БД, события на файловых ресурсах, активность пользователей, активность сетевого трафика, и.т.д). Данная система должна быть настроена согласно установленным стандартам и должна вести обязательный учёт данных о состоянии ИБ – управлять этими данными, журналировать и каталогизировать события собранных из логов корпоративных фаерволлов или ips-систем, сервисных логов, сигнатурных данных с антивирусов, итд. Здесь можно и охватить контроль взаимодействия с сетью-аутсорс, так как наш инсайд взаимодействует с ней.
- Что касается инсайда, да и демилитаризованной зоны, то тут необходимо также внедрить иные инструменты защиты от НСД, которые могли бы помочь с контролем процедур идентификации и аутентификации пользователей, маскировкой и целостностью конфиденциальной информации, доступом к периферийному оборудованию, осуществлением криптозащиты информации, защитой материальных носителей от нелегитимного ввода/вывода информации, гарантированной очистки информации и бэкапирование последней.

И в заключение, хотелось бы отметить то, что важно понимать, что внедрение соответствующих СЗИ и их взаимодействие, должно происходить без конфликтов и конечно же не мешать, и не отсекать излишне пользовательский траффик, и как следствие, задуматься о тех мощностях, которые позволили бы равномерно распределить нагрузку и позволить всем легитимным пользователям беспрепятственно получать доступ ко всей необходимой информации.

Так как, в конечном итоге, именно наличие пользователя-клиента определяет успешность бизнеса.

//Done… ☺