



Структуру уже описанной ранее системы оставлю, выделю дополненную информацию.

Данная ИС состоит из 3х зон (Интернет, DMZ заказчика и Inside заказчика). Представляет из себя виртуальный магазин, с аутсорсной поддержкой систем и кучей клиентов. Т.к. это магазин, значит данная ИС имеет большой спектр информации о клиентах и пр., что говорит нам сразу о чувствительной информации (персональные данные, данные о продукции , которая может составлять коммерческую тайну и пр.)

В связи с вышесказанным, на данную систему мы должны наложить соответствующие требования, согласно законодательству РФ в области защиты информационной безопасности (федеральные законы, руководящие документы ФСТЭК, специальные требования и рекомендации по технической защите конфиденциальной информации) плюс бестпрактисы по международным стандартам ISO 27k.

Есть внешняя сеть с пользователями мобильных устройств и подрядчиком. Подобные подключения должны быть максимально ограничены настройками сетевого оборудования (ASA, Firepower), WAF, IPS и прочими сервисами.

Все события должны собираться в единой системе SIEM для последующей обработки информации для прогнозирования угроз. В дополнение система поможет выявить кибератаки и нарушения политик безопасности.

Полное разграничение прав доступа ко всем системам.

Все незащищенные порты при обменах необходимо перевести на зашифрованные и кастомные.

Защитить ПДн и ИСПДн с применением СКЗИ.

**Т.к. у нас используются облачные сервисы, необходимо обеспечить ИС централизованным управлением и придерживаться стандартам best practice.**

**Необходимо обеспечивать безопасность виртуальных сетей, гипервизоров, изолированных данных.**

**В случае использования BigData существуют риски мошенничества, потери данных, нарушения конфиденциальности данных. Необходимо проводить периодические мониторинги и аудиты.**

**В качестве защиты Вэб сервисов и мобильных приложений необходимо использовать криптографию и шифрование данных, экранирование данных, многофакторную аутентификацию.**

Заранее задуматься о защите от DDoS. Потому что можно получить от конкурентов такой вот подарок под новый год.

Не забываем развернуть сервер резервного копирования, тем более у нас там есть боевые БД.

Не забываем про использование антивирусной защиты как на серверных системах, так и на клиентских.

PBX систему и серверные системы держим в актуальном состоянии. Но не забываем про анализаторы кода во избежание схватить эксплойты.

Периодические мониторинги, пентесты и нагрузочные тестирования защищенности придадут нам уверенности, спокойствия и здоровый сон. 😊