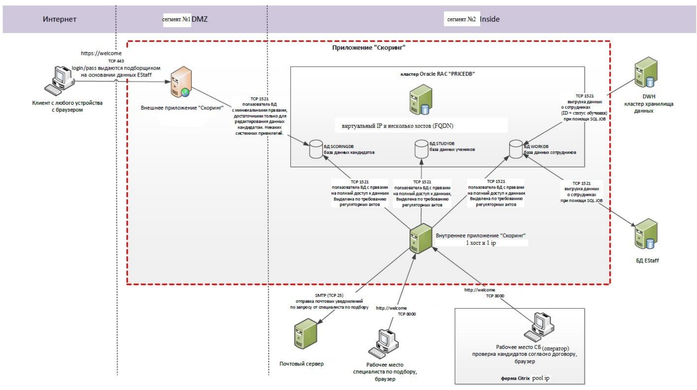
ДЗ №04 - Денис

Урок 4. Информационные системы обеспечения информационной безопасности и средства защиты.
(Часть 1)

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 текущего урока..



Рекомендации сведем в предложенную табличку:

Направления менеджмента	Возможные инструменты реализации\рекомендации по применению
Защита внешнего периметра	WAF - для фильтра запросов извне, особенно важно фильтровать на спецсимволы и попытки брутфорса, подозрительных IP
Защита внутренних сетевых сервисов и информационных обменов	Сегмент DMZ: WAF как реверс-прокси для фильтра подозрительных внутренних запросов для исключения SQL-инъекций, внимание лексическому, поведенческому и анализу регулярных выражений. Здесь же рекомендуется AV: файловый, веб, а так же DLP - для контроля утечек, анализа доступа к информации. Сегмент INSIDE: Сканнер уязвимостей с фокусировкой на сетевые сервисы и протоколы. Обязательный антивирус: почтовый, антиспам. DLP - для контроля утечек, анализа доступа к информации.
Защита серверов и рабочих станций	Антивирус: файловый, проактивная защита - глубокая проверка, подробный отчет. Сканнер уязвимостей с фокусировкой на безопасность ОС, приложений.
Защита информационной инфраструктуры удаленных офисов	WAF: с фокусом на защиту пользователя - в зависимости от приложения, DLP: контроль доступа к чувствительной информации, копирование на носители, ксерокопии, AV: почта, веб, файлы рабочей машины.
Защита системных ресурсов и локальных приложений на серверах и рабочих станциях	Антивирус: файловый, проактивная защита - глубокая проверка, подробный отчет. Сканнер уязвимостей с фокусировкой на безопасность ОС, приложений, сетевых сервисов, безопасность исходного кода.
Защита выделенных сегментов и интеграционных туннелей	WAF, DLP
Защита чувствительной информации всех компонентов IT-ландшафта	AV - контроль угроз веб-соединений, внедрения, почтовые отправления, носители информации. DLP - строгая настойка контроля копирования, носителей, email и социальных сетей Сканнер уязвимостей с фокусировкой на инфраструктуру, сетевые сервисы, приложения.

Задание выполнено!

2020.11.10 15:57