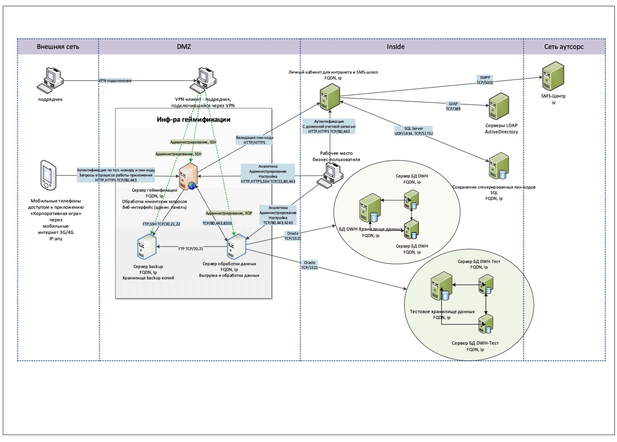
ДЗ №05 - Денис

Урок 5. Информационные системы обеспечения информационной безопасности и средства защиты. (Часть 2)

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..



Сразу сведем в табличку:

Наименование средства защиты	Цели, прикладное размещение и необходимость использования
SIEM	Данной инфраструктуре рекомендуется внедрение SIEM, для оптимизации управлением инцидентами ИБ, снижению рисков + обеспечение стабильности и непрерывности БП. Внедрение позволит эффективно отслеживать и анализировать: контроллеры домена, события на файловых ресурсах, события в БД, события антивируса, активность пользователей, активность сетевого трафика, события syslog. Внедрение необходимо оценить и согласовать с возможностями выделенного бюджета. В случае ограниченного бюджета сделать акцент на наиболее уязвимые и ценные для злоумышленника объекты инфраструктуры (например БД с ценной информацией), файловый сервер (документы/чертежи итд).
SOAR	Внедрение SOAR обеспечит экономию времени за счет автоматизации рутинных процессов, масштабируемость. Визуализация, более качественная аналитика и прогнозирование. Целесообразность зависит от бюджета и целей, роста инфраструктуры компании, оценки рисков.
IPS	Если невозможно внедрить SIEM, можно внедрить практики IPS/IDS для предотвращения и прогнозирования угроз, частичной автоматизации. Однако в большой инфраструктуре это может быть менее эффективно, потребуется больше времени на реагирование. IPS включает модули IDS(детектирование угроз, анализ траффика до уровня L7) и помогает быстрее реагировать, автоматизировать, предотвратить атаки, прогнозировать, настроить триггеры, сфокусировать защиту важных объектов.
IDS	Детектирование угроз, работает в паре с IPS. Данной инфраструктуре рекомендуем внедрение как APIDS так и NIDS на все сервера DMZ и INSIDE.
Инструменты защиты от НСД	Рекомендуется внедрение/оптимизация для защиты от НСД в данной инфраструктуре: • Процедуры идентификации и аутентификации. • Обеспечение мандатного и дискретного контроля доступа. • Защита ввода\вывода на материальный носитель. • Маркировка конфиденциальных документов. • Регистрация событий безопасности в логах. • Использование криптографии и шифрования. • Контроль целостности конфиденциальной • Контроль доступа к периферийному оборудованию.

Задание выполнено!

2020.11.11 04:11