Выполнил: Самхарадзе Г.Т

Условие:

У Заказчика есть ГИС с классом защищенности К3.

ГИС размещена в виртуальной инфраструктуре, которая имеет подключение к сетям общего пользования посредством кластера маршрутизаторов Cisco ASR.

Пропускная способность каналов связи с сетями общего пользования составляет 2 Мбит/с.

В ГИС используется межсетевой экран (далее - МЭ) FortiGate для сегментирования и фильтрации трафика при взаимодействии ГИС с сетями общего пользования и внутрисегментном взаимодействии.

В ГИС имеются следующие сегменты:

1. Сегмент демилитаризованной зоны, в нем размещены веб-серверы, почтовый релей, сервер обновления антивирусных баз;
2. Серверный сегмент, в нем размещены серверы приложений, серверы баз данных ГИС;

3. Пользовательский сегмент, в нем размещены АРМ пользователей;

4. Сегмент управления, в нем размещены сервер управления МЭ FortiGate и сервер управления антивирусным ПО.

Необходимо подобрать решение по защите от атак типа «отказ в обслуживании».

Для этого требуется:

1. Подготовить обоснование для внедрения решения типа «отказ в обслуживании» с отсылкой на требования регуляторов в области ИБ в РФ;

2. Подготовить эскизное описание и схему технического решения по защите от атак типа «отказ в обслуживании» и его интеграции в инфраструктуру ГИС.

Решение по защите от атак типа «отказ в обслуживании» должно в том числе обеспечивать противодействие распределенным атакам на отказ в обслуживании с превышением пропускной способности внешних каналов связи и пограничного оборудования ГИС.

Решение:

1) Атаки типа «отказ в обслуживании» способны нарущить функционирование практически любой информационной системы, особенно в случаях отсутствия защиты от данного типа атак и в случаях высокого уровня технической оснащенности и подготовки злоумышленников. Так как в рамках данного технического решения речь идёт о ГИС, то актуальность угроз подобного рода и их опасность возрастает в разы, из чего следует очевидность необходимости внедрения решения по отражению атак типа «отказ в обслуживании». Так же подкрепить необходимость данного решения можно методическим документом

ФСТЭК(3.10 Обеспечение доступности информации. ОДТ1 Использование отказоустойчивых технических средств стр.95)

2) Для достижения наиболее эффективного результата в изначальную архитектуру представленной системы были внесены некоторые изменения:

В первую очередь была добавлена сама система защиты от DDoS аттак и в данном случае выбор пал на Radware DefensePro, в силу того, что данное решение так же обеспечивает защиту от большинства IoT-ботнет аттак в реальном времени, а так же от большинства известных и выявленных угроз (так же у данной системы есть огромный ряд других преимуществ, с которыми можно ознакомиться на самом сайте Radware)

Для защиты от атак на переполнение каналов связи был введён модуль DefensePipe, который как и предыдущее решение является продуктом компании Radware

Для защиты от веб-аттак были приняты достаточно классические меры в виде введения фаервола WAF

Помимо принятых технических мер, так же был добавлен балансировщик нагрузки.

Стоит отметить, что так же предполагается, что все вышеперечисленные решения будут работать в рамках единой системы и так же предполагается наличие команды специалистов, оперативно реагирующих на возможное возникновение неполадок в рамках данной системы.