Домашнее задание 2
Информзащита стажировка

Самхарадзе Г.Т.

Выбор направления/решения из лекции, прошедшей 18.03.2021

«Безопасность прикладных систем» и пояснение выбора данного направления.

В рамках данного домашнего задания было принято выбрать в качестве описываемого решения WAF(web application firewall, есть сразу несколько причин почему было выбрано именно данное решение
-В наше время число компаний, которые применяют веб-технологии растёт практически с каждым годом, так же в многочисленных отчётах(например, «Global Internet Security Report» от компании Symantec) можно найти информацию о том, что как показывают статистика и практика, киберпреступники при взломе веб-сайтов например, обычно используют как раз таки уязвимости веб-приложений, так же киберпреступники любят использовать уязвимости ОС, на которой работают эти приложения(в качестве примеров атак можно привести атаки типа XSS или же SQL-иньекции), считается что данная проблема как никогда актуальна в наши дни и из всего возможного множества решений(Firewall, IPS/IDS, NGFW,WAF) только WAF способен обеспечить необходимую защиту веб-приложений от известных и неизвестных угроз, помимо этого WAF соответствует требованиям регуляторов, например стандартам PCI DSS.

-WAF является достаточно популярным решением на рынке уже много лет, он включает в себя все возможные классические методы защиты для решений подобного типа, но помимо этого способен использовать и уникальные подходы
-Сравнивая WAF с тем же NGFW, можно сказать,что архитектура WAF позволяет анализировать целиком кажыдй сеанс связи и в целом позволяет выполнять более точный поведенческий анализ, в следствие этого WAF лучше выявляют отклонения в нормальной работе приложений и могут противостоять уязвимостям нулевого дня.

-С известными уязвимостями WAF так же способено бороться оригинальным образом, благодаря технологии патчинга, которая позволяет WAF закрыть брешь, не дожидаять выхода обновления компонента

-WAF так же способен решать достаточно важную проблемы избыточности(запросов и логов), это происходит за счёт выявления корреляций между ними и обьединения взаимосвязанных сообзений в цепочки, это позволяет увидеть развитие атаки и быстро среагировать на неё.

-Статистически рост рынка WAF за 2015 год как минимум составил 30%, так же предполагается что с каждым годом данная цифра будет лишь увеличиваться, что говорит о доверии к данному продукту в рамках корпоративного сегмента и сегмента информационной безопасности.

-WAF система узкоспециализированная и работает она только с протоколами HTTP/HTTPS, это можно было бы представить в качестве минуса, если бы количество данных протоколов не было настолько велико, ведь в данном случае они действительно нуждаются в специализированном средстве.

Описание решения

В качестве конкретного продукта будет рассматриваться Imperva SecureSphere WAF. Данное решение от компании Imperva способно обеспечить достойную защиту за счет одновременного применения следующих технологий :

-сигнатурный анализ

- проверка протоколов на аномалии

-отслеживание сессий

- динамическое профилирование

Представленное решение успешно противодействуют как всем атакам из OWASP-TOP10, так и другим менее известным, но более изощренным. Устройства обладают возможностями по инспектированию зашифрованных данных, пересылаемых по протоколу SSL (HTTPS). Решение состоит из следующих модулей:

-SecureSphere WAF - защита веб-приложений от кибератак

-ThreatRadar - репутационная база данных.

Secure-Sphere WAF глубоко анализирует логику работы веб-приложения, выполняет интеллектуальное исследование попыток проникновения и атак. Решение оснащено механизмом защиты от червей и других вредоносных атак на веб-серверы и приложения, основу которого составляют механизмы на основе сигнатур популярной системы Snort и собственных SQL-сигнатур, разрабатываемых исследовательским центром ADC (Application Defense Center) самой компании Imperva. Встроенный межсетевой экран осуществляет надежную защиту от неавторизованных пользовательских запросов и атак на сетевом уровне.

Так же предустановленные в системе отчеты полностью удовлетворяют требованиям стандартов информационной безопасности. Возможно создание пользовательских отчетов и экспорт в различные форматы. Дополнительные облачные сервисы позволяют упростить безопасность и справится с DDoS-атаками. Важным преимуществом устройств SecureSphere WAF является наличие уникального сервиса ThreatRadar, обеспечивающего защиту от автоматизированных атак. Благодаря быстрому получению достоверной информации об источниках атак, ThreatRadar позволяет немедленно блокировать трафик, идущий от подозрительных

источников, еще до момента осуществления какого-либо разрушительного действия. Решения Imperva отличаются прозрачной поддержкой и простым развертыванием. Ниже представлена схема применения описываемых решений:

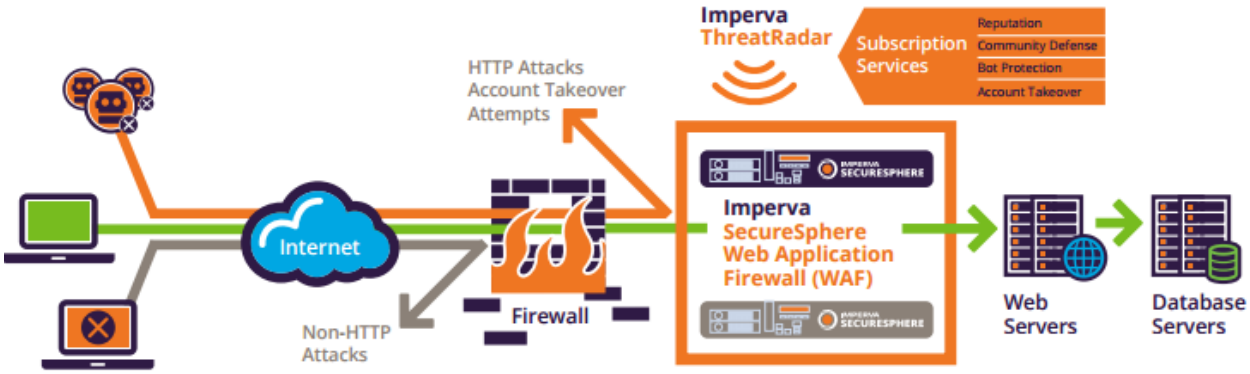

Рис 1. Схема применения Imperva WAF и ThreatRadar

Возможности интеграции данного продукта представлены ниже:

Сканеры уязвимостей(WhiteHat, IBM, Cenzic, NT OBJECTives, HP, Qualys, Beyond Security)

Системы контроля БД(Imperva SecureSphere Database Activity Monitoring, Imperva SecureSphere Database Firewall)

Антивирусы(FireEye, Proofpoint Threat Response)

SIEM(HPE ArcSight, RSA enVision, Splunk, IBM Qradar)

Anti-fraud(ThreatMetrix Cybercrime Defender Platform)

DLP(Imperva SecureSphere File Activity Monitoring)

Threat intelligence(Imperva Threat Radar)

Защита от DDoS(Imperva Incapsula)

Касаемо возможной области применения данной системы защиты и данного решения, она достаточно широка в рамках рассматриваемого вопроса, данная защита может быть применима и полезна как для бизнес-решений разного уровня, представленных в виде веб-приложений, так и для информационных систем другого рода, нуждающихся в защите подобного рода.

Заключение

В ходе аргументации выбора решения в самом начале данной работы уже были приведены все необходимые аргументы и предпосылки для интеграции решений типа WAF в защиту тех или иных процессов, помимо этого так же был рассмотрен вопрос актуальности и необходимости данного решения, все технические аспекты и преимущества рассмотреть не представляется возможным, ибо их достаточно большое количество не позволит уложиться в выделенный формат, однако, подводя итоги можно сказать, что решения типа WAF покрывают достаточно большое количество актуальных проблем в области ИБ(например защита XML и HTTP траффика, мониторинг аттак, защита от широкомасштабных аттак, защита на сетевом, сервисном и прикладных уровнях, защита от аттак типа «отказ в обслуживании», защита от ботов, анализ событий безопасности, тарификация и.т.д). Преимущества решений типа WAF перед другими так же были описаны в первом пункте, в любом случае можно заключить, что данный тип решений является как минимум интересным для рассмотрения, анализа и в некоторых случаев возможно даже необходимым для применения, за счёт своего функционала и преимуществ перед другими решениями, пытающихся покрыть те же проблемы в рамках ИБ.