УДК 004.056

РАЗРАБОТКА И ВНЕДРЕНИЕ МОДЕЛИ БРАНДМАУЭРА ВЕБ-ПРИЛОЖЕНИЙ НА ОСНОВЕ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

Галанц Ю.В. (Санкт-Петербургский государственный университет информационных технологий, механики и оптики),
Научный руководитель – к.т.н., доцент Менщиков А.А.
(Полное название организации)

Атаки на веб-приложения набирают популярность, поскольку позволяют нарушителям использовать доверенные веб-ресурсы в качестве базы для размещения своего вредоносного ПО или проводить иные атаки в отношении клиентов компании. В данном исследовании была предложена гибридная модель брандмауэра веб-приложений с использованием машинного обучения для предотвращения веб-атак основываясь на анализе сигнатур и обнаружении аномалий.

Введение.

Мы живем в эпоху постоянного роста влияния информационных технологий на все сферы жизни человечества. Интернет – один из важнейших инструментов современного общества. С его развитием начали появляться огромные множества веб-приложений, что в свою очередь открыло перед нами как новые возможности, так и новые угрозы.

Основной метод воздействия на веб-приложение – HTTP запросы. Целью данного исследования стало создание модели брандмауэра веб-приложений, сочетающего в себе сигнатурный анализ, поиск аномалий и машинное обучение.

Было запланировано обеспечить продукт функционалом позволяющим обнаруживать SQL инъекции, XSS атаки и атаки с обходом каталогов.

Основная часть.

Главной задачей стал подбор оптимального сочетания методов машинного обучения для создания модели обнаружения аномалий в HTTP запросах в комбинации с сигнатурным анализом на основе уже известных уязвимостей.

В ходе работы был собран набор данных для обучения нейронной сети, разработан интерфейс брандмауэра и необходимый функционал. Был поставлен эксперимент, подразумевающий проведение атак на машину-жертву с установленным разработанным брандмауэром, и сняты показания. По результатам анализа эксперимента были проведены доработки для улучшения показателей работы созданного продукта.

Выводы.

Полученную разработку можно использовать для повышения общего уровня безопасности веб-серверов и приложений. Основываясь на результатах, полученных в ходе проведения исследования, были сделаны выводы о дальнейшем развитии изучения затронутой темы.

Галанц Ю.В. (автор)

Менщиков А.А, (научный руководитель)