УДК 004.056.52

ВНЕДРЕНИЕ МЕЖСЕТЕВОГО ЭКРАНА УРОВНЯ ПРИЛОЖЕНИЙ НА ПРЕДПРИЯТИИ

Н.А. Приходченко

Учреждение образования «Гомельский государственный университет имени Франциска Скорины», г. Гомель, Республика Беларусь

Аннотация. В данной статье рассматривается процесс выбора и внедрения межсетевого экрана уровня приложений (WAF) как критического компонента системы защиты современных веб-сервисов. Выделены основные трудности, с которыми сталкиваются предприятия при подборе средств защиты, включая разнообразие доступных на рынке решений и специфику нормативно-правовой базы Республики Беларусь. Описан пошаговый алгоритм, учитывающий соответствие техническим регламентам, особенности ИТ-инфраструктуры и квалификацию персонала предприятия. Практическая значимость работы заключается в систематизации этапов выбора, пилотного тестирования и настройки WAF для минимизации рисков и оптимизации затрат ресурсов.

Ключевые слова: межсетевой экран уровня приложений; WAF; информационная безопасность; веб-приложение; кибератака; алгоритм внедрения; ТР 2013/027/BY; фильтрация трафика; пилотное тестирование; защита данных.

IMPLEMENTATION OF A WEB APPLICATION FIREWALL AT AN ENTERPRISE

N.A. Pryknodchenko
Educational Institution "Francysk Skaryna Gomel State University", Gomel, Republic of Belarus

Abstract. This article examines the process of selecting and implementing a Web Application Firewall (WAF) as a critical component of modern web service security systems. It highlights the key challenges enterprises face when selecting security solutions, including the diversity of solutions available on the market and the specifics of the regulatory framework of the Republic of Belarus. A step-by-step algorithm is described, taking into account compliance with technical regulations, IT infrastructure features, and staff qualifications. The practical significance of the work lies in the systematization of WAF selection, pilot testing, and configuration to minimize risks and optimize resource costs.
Keywords: Web Application Firewall; WAF; information security; web application; cyberattack; implementation algorithm; TR 2013/027/BY; traffic filtering; pilot testing; data protection.

Введение

На данный момент веб-приложения стали неотъемлемой частью современной информационной инфраструктуры. Также из-за своей выросшей важности они стали частой целью для кибератак, вследствие чего появилась острая необходимость в создании надежной системы защиты. Неотъемлемой частью такой системы является межсетевой экран уровня приложений (WAF) является неотъемлемым компонентом системы защиты веб-приложений. Этот инструмент выполняет фильтрацию HTTP/HTTPS трафика между сервисом и пользователем, защищает от ряда разновидностей атак, а также защищают сервисы API. Однако, несмотря на необходимость данного инструмента для безопасной работы приложений, выбор и внедрение межсетевого экрана уровня приложений на предприятии может стать сложной задачей для неподготовленных сотрудников. Эти трудности вызваны в первую очередь большим разнообразием вариантов WAF, доступных на рынке, а также особенностями его внедрения и сопровождения.

В этой статье описывается алгоритм выбора и внедрения WAF, призванный облегчить данные процессы для руководства и сотрудников фирм и предприятий.

Основная часть

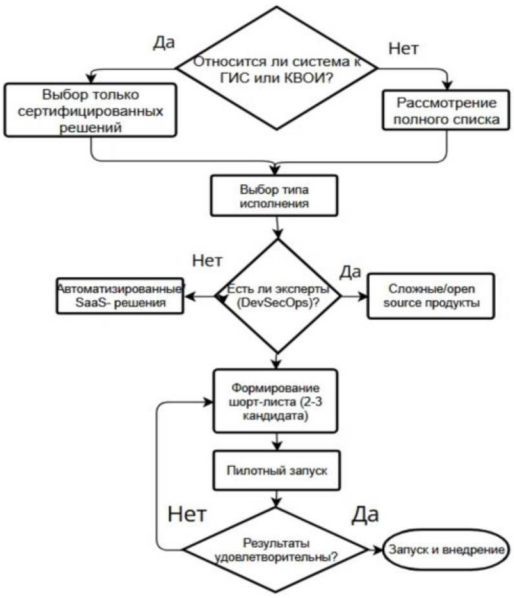
В первую очередь при выборе межсетевого экрана уровня приложений необходимо обеспечить соответствие нормативно-правовым документам в области информационной безопасности Республики Беларусь. Если защищаемая информационная система относится к критически важным объектам информатизации либо к государственным информационным системам (ГИС), то средства защиты должны иметь действующий сертификат соответствия требованиям Технического регламента ТР 2013/027/BY. В случае, если веб-приложение не относится к вышеуказанным информационным системам, наличие сертификата не является необходимым.

Вторым шагом будет рассмотрение архитектуры предприятия и наиболее вероятных угроз. Именно на этом этапе определяются желаемые характеристики WAF. Принятие решения на данном этапе во многом зависит от особенностей инфраструктуры, функций и вида деятельности конкретного предприятия.

На третьем этапе оценивается структура предприятия и его кадровый состав. Для большинства программных и аппаратных вариантов WAF необходимо наличие в штате квалифицированных специалистов, способных выполнить сопровождение и мониторинг во время работы системы защиты. В случае, если отдел информационной безопасности отсутствует либо не способен выполнить эту задачу, следует прибегнуть к использованию облачных межсетевых экранов, в случае которых сопровождение берет на себя провайдер услуги.

Заключительным этапом выбора WAF является пилотное тестирование. На этом шаге также начинается процесс внедрения межсетевого экрана в инфраструктуру предприятия. Непосредственно перед пробным запуском проводится подготовка среды. В течение срока от двух недель проводится тестирование WAF в режиме мониторинга, в ходе которого производится настройка и определяется эффективность работы средства защиты. Когда количество ложных срабатываний будет сведено к минимуму, WAF постепенно переводится в режим блокировки и интегрируется в существующую систему защиты предприятия. К этому моменту, как правило, уже принято окончательное решение о приобретении и внедрении межсетевого экрана. В случае, если в ходе пилотного тестирования средство защиты было признано неподходящим для предприятия, начинается повторный выбор продукта. Заключительным этапом внедрения является разработка регламентов эксплуатации, мониторинга и реагирования.

Основные шаги алгоритма представлены на рисунке.



Алгоритм выбора WAF для последующего внедрения на предприятии
Algorithm for WAF selection and subsequent enterprise implementation

Заключение

Из работы следует, что выбор WAF для последующего внедрения является сложной и комплексной задачей, требующей вдумчивого подхода и тщательного рассмотрения функций, рода деятельности, внутренней структуры и ресурсов предприятия. Внедрение неподходящего продукта может повлиять на работу всей инфраструктуры, снизить производительность работы либо привести к значительным финансовым и трудовым затратам. Представленный алгоритм выбора и внедрения должен облегчить выполнение данных задач и сэкономить ресурсы, которые в ином случае были бы потрачены напрасно.

Сведения об авторах

Приходченко Н.А., студент факультета физики и информационных технологий специальности «Компьютерная безопасность», Учреждения образования «Гомельский государственный университет имени Франциска Скорины», mbirann@gmail.com.

Information about the authors

Prykhodchenko N., student of the Faculty of Physics and Information Technology specialty "Computer security", Educational Institution "Francysk Skaryna Gomel State University", mbirann@gmail.com.