В.М.АЛЕФИРЕНКО[1], К.В.ЧОПИК[1]

УГРОЗЫ БЕЗОПАСНОСТИ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЕ ИНТЕРНЕТ-МАГАЗИНА

[1]*Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», г. Минск, Республика Беларусь*

Интернет торговля, на сегодняшний день, самый популярный способ совершения покупок, которому отдает предпочтение множество покупателей. Вместе с активным ростом и развитием таких площадок, растет интерес к интернет-магазинам со стороны киберпреступников. Интернет-магазины – привлекательная мишень для кражи информации и получения незаконной прибыли от выполнения «заказов» недобросовестных конкурентов ресурса. Для получения информации киберпреступники могут использовать следующие типы атак [1]:

– атака Man In The Middle;
– DoS-атака;
– Reply-атака.

Совершая покупки в интернет-магазинах, пользователи передают большой объем персональных и финансовых данных, хищение которых представляет интерес для киберпреступников. Для завладения такими данными используется заражение вирусным кодом интернет-магазина или перенаправление на поддельные фишинговые сайты.

Одной из самых популярных атак на информационную инфраструктуру интернет-магазина является внедрение вредоносного кода в программную платформу. Оно отрицательно влияет на работоспособность и рейтинг интернет-магазина в поисковых системах. При внедрении в программный код сторонних ссылок, киберпреступники осуществляют перенаправление пользователей интернет-магазина на сторонние, конкурентные или поддельные фишинговые сайты.

В результате заражения замедляется работа, появляются ошибки, пустые окна, посторонний текст и реклама. Поисковые системы самостоятельно обнаруживают угрозы внутри сайта, после чего относят его к потенциально опасным, вносят в свои «черные списки» и не отображают при запросах пользователей.

Для повышения надежности работы интернет-магазина и минимизации ущерба от потенциально проведенной атаки необходим комплексный и превентивный подход к вопросам безопасности. Одной из таких необходимостей является использование антивирусных средств, регулярное обновление их модулей и баз, выполнение резервного копирования данных, отслеживание за настройкой веб-сервера с открытием функций и прав доступа только в объеме, необходимом для работы интернет-магазина, использование сложных паролей доступа и регулярное их обновление. Регулярная процедура проведения аудита безопасности информационной системы интернет-магазина позволяет оценить зрелость системы управления информационной безопасности и выявить уязвимости для их оперативного устранения.

Применение многоуровневой защиты интернет-магазина помогает значительно повысить устойчивость к атакам киберпреступников и проникновению вредоносного программного средства на сайт. Такая защита достигается путем внедрения дополнительных барьеров в виде сетевых экранов, фильтрующих и проверяющих входящий интернет-трафик.

Защита интернет-магазина должна включать комплекс непрерывных, постоянно действующих и развивающихся мер. Высокий уровень защиты интернет-магазина от внешних угроз помогает предотвратить и минимизировать потенциальные риски простоя, падения рейтинга и потери репутации. Следует всегда помнить, что повышенное внимание к безопасности – это прежде всего вклад в успешное функционирование и развитие бизнеса.

ЛИТЕРАТУРА

1. Алефиренко, В. М. Угрозы безопасности информационной инфраструктуре объектов различного назначения / В.М. Алефиренко, К.В. Чопик // Znanstvena misel journal. – 2019. – Vol. 1, № 30. – С. 41 – 49.