В современном мире популярность интернет – магазинов достигла очень высокого уровня. Огромное количество людей, ежедневно, совершают онлайн покупки: еда, одежда, техника, товары для дома и прочее.

Но, как мы знаем, всё, что находится в сети, подвержено различным угрозам. Оформляя заказы в интернет – магазинах, мы предоставляем свои конфиденциальные данные, не задумываясь о том, надежно ли они защищены.

Существует ряд угроз, которым может быть подвержен интернет – магазин:

1. DDoS – атаки – процесс, при котором сайт выводится из работы, тем самым, люди попадают на неработающий сайт, покидают его и отдают предпочтение конкуренту, чей сайт находится в рабочем состоянии.
2. Вирусные ссылки – путем хакерских действий, на ссылку сайта «вешается» вирус, при входе на такой сайт выскакивает предупреждение о небезопасности, а сам сайт отправляется в черный список для посещения.
3. Подмена информации сайта – изменяются характеристики, описание, цена товаров, возможно, ссылки направляют на другие источники продажи, тем самым покупатель считает магазин ненадежным.
4. Кража конфиденциальных данных – база личных данных покупателей, включая ФИО, адрес, данные карты, находятся в руках мошенников и могут быть использованы в самых разных целях.
5. Атаки на этапах оплаты товара – путем хакерских действий, может быть «пропущен» этап оплаты товара и сразу же осуществляется этап сбора и доставки товара.

Такие угрозы могут быть осуществлены при условии, если в написании кода для интернет– магазина есть «дыры», в которые могут проникнуть хакеры. Слабая система безопасности, которая допускает вирусы и DDoS – атаки.

Действия, которые нужно предпринять, чтобы не допустит вышеописанных ситуаций:

1. Нанять в штат грамотного ИТ специалиста, отвечающего за информационную безопасность

2. Проводить личные проверки, с помощью специальных сервисов по DDoS - атакам
3. Установить файрвол/брандамауэр
4. Установка системы по анти DDoS защите
5. Установка SSL сертификата
6. Не устанавливать легких паролей
7. Делать бэкап
8. Не экономить на оборудовании, предназначаемого для защиты системы.

Из всего вышесказанного можно сделать вывод, что только комплексные действия могут защитить работу интернет – магазинов, но нельзя быть на 100% уверенным, что, если, будет установлено самое дорогое оборудование и один раз проведена проверка, то все под контролем. Проверки должны проводиться на постоянной основе и своевременно.

Самый популярное решение на сегодняшний день – передать процесс защиты от DDoS и хакерских атак на интернет – магазин на аутсорсинг. Такой подход действительно может довольно недорого решить проблемы безопасности. Методы атак, которые уже известны и которые не учитывают специфику интернет - магазна, будут отражены достаточно эффективно. Именно из-за бурного развития таких сервисов многие типы атак сошли на нет, а новые алгоритмы атак появляются не так часто, и хакеры их придерживают для атак на заметные или денежные объекты. Так что к тому времени, как новый тип атаки дойдет до небольшого интернет-магазина, алгоритмы противодействия ему, скорее всего, будут уже найдены и будут использоваться в большинстве облачных средств защиты.