ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ЭЛЕКТРОННОМ БИЗНЕСЕ

Деркач А.В., Ахрамейко П.Д., Каминская М.М.

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Ермакова Е.В. – канд. экон. наук

Сегодня глобальная телекоммуникационная сеть Интернет оказывает существенное влияние на все экономические структуры, помогая предприятиям снижать материальные затраты, по-новому строить отношения с партнерами, выходить на новые рынки поставок и сбыта, создавать дополнительные источники дохода. Можно без преувеличения сказать, что Интернет становится средой ведения активного бизнеса.[1] Одним из ключевых моментов эффективного использования электронного бизнеса является его информационная безопасность. В данной работе рассмотрены виды угроз, способы и средства защиты от данных угроз.

Безопасность — это состояние, при котором отсутствует возможность причинения ущерба потребностям и интересам субъектов отношений. Применительно к электронной коммерции определение безопасности можно сформулировать как состояние защищенности интересов субъектов отношений, совершающих коммерческие операции с помощью технологий электронной коммерции, от угроз материальных и иных потерь.

Угрозой информации называют потенциально возможное влияние или воздействие на автоматизированную систему с последующим нанесением убытка чьим-то потребностям. Угрозы информационной безопасности проявляются не самостоятельно, а через возможное взаимодействие с наиболее слабыми звеньями системы защиты, то есть через факторы уязвимости. Угроза приводит к нарушению деятельности систем на конкретном объекте-носителе.

Наиболее серьезными угрозами в области информационной безопасности (ИБ) сайтов и веб-приложений компаний сейчас являются следующие:

- изменение информации, размещенной на веб-страницах, в том числе замена главной страницы сайта на другую (дефейс);

нарушение работоспособности и доступности интернет-ресурсов (например, в результате DDoS-атак);

- массовое несанкционированное скачивание информации с веб-страниц сайтов (веб-скрейпинг);

- проникновение внутрь информационных систем организации;

- использование сетевых и серверных ресурсов компании для реализации замыслов злоумышленника (например, рассылки спама, распространения вредоносных кодов и пр.);

- кража конфиденциальной информации (например, персональных данных);

- воздействия различного рода с целью мошенничества (fraud);

- мошенничество.

Для компаний электронной коммерции наиболее чувствительными являются направленные атаки, целью которых является получение доступа к персональным данным клиентов, различные виды мошенничества, веб-скрейпинг (scraping) и DDoS-атаки.[6]

Основными объектами целенаправленных атак на компании электронной коммерции являются мобильные приложения, корпоративные веб-приложения, «классические» браузерные приложения, интерфейсы для взаимодействия между сервисами внутри компании и с сервисами партнеров (API-интерфейсы), а также атаки могут быть направлены на сети, внутри которых развернуты приложения и инфраструктура их предоставления.[2]

Если говорить о компаниях, опасности и потенциальные киберпреступления намного превосходят их готовность противодействовать атакам. Порядка 63% компаний не имеют никаких процедур или планов действий на случай их возникновения. Опрос организаций на наличие систем безопасности показал, что такие системы применяют 37% организаций, 12% имеют системы, но не используют её. Что касается остальных организаций, составляющие 51% из общего числа, у них отсутствует система мероприятий по борьбе с кибератаками. В итоге получаем, что, сотрудничая с какой-либо организацией, шанс быть защищенными при кибератаке составляет около 50%.[5]

В связи с широким спектром уязвимых мест в электронной коммерции система должна отвечать четырем основным требованиям:

1. Конфиденциальность – обмен информацией должен быть защищен от посторонних лиц.

2. Целостность – передаваемая информация не должна быть изменена или подделана.

3. Проверка подлинности – как отправитель, так и получатель должны доказать свою подлинность друг другу.

4. Невозможность отказа – после совершения операции каждая сторона должна получить подтверждение о состоявшейся сделке

получить подтверждение о состоявшейся сделке

Для обеспечения безопасности электронной коммерции приложения и сайты должны иметь как внутреннюю систему безопасности, так и внешнюю.

На стадии проектирования архитектуры сайта или приложения следует придерживаться рекомендаций консорциума ISTF (Internet Security Task Force). Согласно рекомендациям, создатели электронного бизнеса в первую очередь должны обратить внимание на ряд таких областей информационной безопасности, как аутентификацию, определение атак, контроль доступа, контроль за потенциально опасным содержимым, администрирование, обеспечение конфиденциальности информации и другие области.[3]

Создаваемый электронный бизнес должен быть спроектирован с возможностью подключения внешних сервисов, обеспечивающих защиту от возможных угроз и атак, и включать следующие процессы: управление уязвимостями, конфигурациями и инцидентами, мониторинг и аудит.

Рекомендуется внедрять сервисы, включающие облачные возможности защиты от DDoS-атак (anti-DDoS) и также функционал интеллектуальных межсетевых экранов уровня веб-приложения (Web Application Firewall, WAF). Сервисы anti-DDoS должны обеспечивать безопасность на уровнях L3 (сетевом), L4 (транспортном) и L7 (уровень приложений) модели OSI. Сервисы WAF предназначены для обеспечения безопасности данных, но не для защиты от DDoS-атак, направленных на переполнение каналов. В связи с этим, необходимо совместное использование указанных сервисов.

Помимо описанных выше мер стоит упомянуть иные методы защиты электронного бизнеса от взлома и мошенничества. Следует:

Размещать сайт на безопасной платформе электронной коммерции.

Использовать безопасные соединения для онлайн-заказов. Для этого необходима совместимость разрабатываемого проекта с PCI (Payment Card Industry Data Security Standard - стандарт безопасности данных индустрии платёжных карт).

Использовать отслеживание номеров всех заказов, которые вы отправляете. Данный метод поможет распознать мошенников, использующих возвратные платежи.

Не хранить конфиденциальные данные пользователей.

Использовать систему проверки адреса и карты.

Установить систему предупреждения о подозрительной деятельности.

Ежеквартально выполнять PCI-сканирование с помощью таких сервисов, как Trustwave, чтобы снизить риск уязвимостей платформы вашей электронной коммерции для атак хакеров.[4]

Вывод:

Следует помнить, что стопроцентной защиты от хакеров и мошенников нет, так как невозможно предусмотреть и обнаружить все возможные уязвимости приложения или сайта, однако их число необходимо минимизировать. Самый простой способ достичь этого – не распространять свою личную информацию. Также рекомендуется постоянно проверять и отслеживать угрозы и инциденты для последующего улучшения безопасности.

Список использованных источников:

1. "ЭЛЕКТРОННЫЙ БИЗНЕС" И НАШЕ БУДУЩЕЕ [Электронный ресурс] - Электронные данные. - Режим доступа: https://logistics.ru/9/22/i20_3025.htm - Дата доступа: 28.02.2022

2. Защита компаний электронной коммерции от интернет-угроз [Электронный ресурс] - Электронные данные. - Режим доступа: https://tproger.ru/articles/zashhita-kompanij-jelektronnoj-kommercii-ot-internet-ugroz/ - Дата доступа: 02.03.2022

3. Обеспечение информационной безопасности сетей [Электронный ресурс] - Электронные данные. - Режим доступа: http://ypn.ru/146/securing-networking-information/2/ - Дата доступа: 03.03.2022

4. О СПОСОБАХ ЗАЩИТЫ ЭЛЕКТРОННОГО БИЗНЕСА [Электронный ресурс] - Электронные данные. - Режим доступа: https://scienceforum.ru/2018/article/2018005279 - Дата доступа: 05.03.2022

5. Масюк, Л. С. Незащищенность клиентов при работе с сервисами электронной коммерции / Л. С. Масюк, Н. А. Михаленок // Проблемы экономики и информационных технологий: материалы 53-й научной конференции аспирантов, магистрантов и студентов (Минск, 02 – 06 мая 2017 г.). – Минск: БГУИР, 2017. – С. 140 – 142.

6. Курейчик, К. П. Основы классификации угроз информационной безопасности информационно-измерительных систем удаленной обработки данных / К. П. Курейчик, А. А. Трушкевич // Доклады БГУИР. - 2011. - № 5 (59). - С. 35 - 41