Угрозы информационной безопасности в ретейле

Positive Technologies

ptsecurity.com

Главные выводы

- За 2020–2021 годы количество кибератак на ретейл выросло на 117% по сравнению с 2018–2019 годами.
- По результатам 2021 года в 70% атак на компании из сферы торговли злоумышленники намеревались получить доступ к важной информации. В первую очередь хакеров интересовали персональные данные (32% от общего объема украденных данных), данные платежных карт (21%), базы данных клиентов (13%) и коммерческая тайна (13%).
- Главные последствия кибератак на ретейл — финансовые потери, репутационный ущерб, штрафы за нарушение законодательства и судебные иски от пострадавших клиентов.
- Доля атак на ретейл с использованием программ-вымогателей в 2021 году выросла на 40 процентных пунктов в сравнении с 2020 годом и составила 79%.
- Примерно в семи из десяти объявлений в дарквебе, касающихся взлома сайтов, основная цель атаки — получение доступа к веб-ресурсу. Больше всего скупщиков интересуют интернет-магазины: цены на доступы к ним варьируются от 50 до 2000 $.
- Большинство недопустимых событий ИБ в ретейле связаны либо с атаками на покупателей, что приводит к утрате доверия клиентов, либо с доступностью сервисов — как сайтов, так и инфраструктуры. В результате реализации любого такого события ретейлер несет серьезные финансовые потери или упускает выгоду.

Растет рынок — растет и число киберугроз

Рынок электронной коммерции растет с каждым годом. Например, в России за 2021 год количество онлайн-заказов выросло на 104%, а объем рынка вырос на 52% по сравнению с 2020 годом, согласно данным исследовательского агентства Data Insight.

Злоумышленники все чаще обращают внимание на преуспевающие компании и отрасли, и сфера торговли не стала исключением. Как правило, атакующие ретейл хакеры преследуют прямую финансовую выгоду или хотят получить доступ к клиентским данным. В последний год аудитория интернет-магазинов значительно выросла. Пользователи оставляют персональные и платежные данные на сайтах, увеличились объемы онлайн-продаж, соответственно, заметно возрос и интерес злоумышленников. Так, в 2021-м число атак на компании этой отрасли составило 3% от общего количества атак за год.

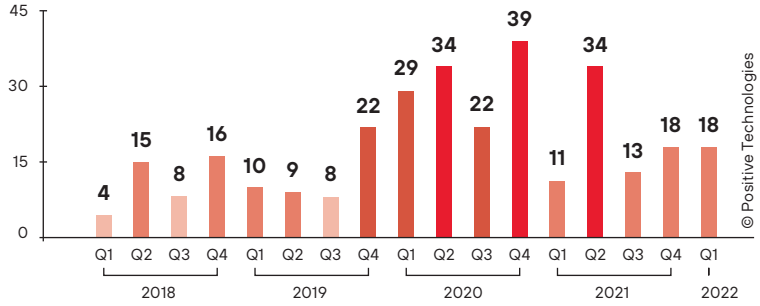

Рисунок 1. Количество кибератак[1] в сфере торговли с Q1 2018 года по Q1 2022 года

За 2020–2021 годы количество кибератак на ретейл увеличилось более чем в два раза (на 117%) по сравнению с 2018–2019 годами.

[1] Масштабные кампании, направленные на большое количество организаций (например, атаки Magecart) в рамках одного квартала, в ходе анализа учитывались как один инцидент.

Чем рискуют магазины

Успех торговли напрямую зависит от клиентов, а значит, реализация любого нежелательного или недопустимого события, затрагивающего покупателей, скажется на бизнесе. К примеру, пошатнуть доверие пользователей могут как новости о краже банковских данных или о хищении денежных средств с их счетов, так и сбои в работе интернет-магазина, потеря заказанного товара. Если же клиенты потеряют доверие к интернет-магазину, то он лишится прибыли и, возможно, обанкротится.

Еще одна составляющая успешного бизнеса — финансовая устойчивость. Одно из существенных для компаний последствий кибератак — финансовые потери. Эта угроза актуальна и для ретейла: к примеру, хакеры могут взломать сайт интернет-магазина и подменить цены дорогостоящих товаров. Если мошеннические действия останутся незамеченными и компания продаст товар по заниженной цене, она понесет убытки.

Как правило, главными последствиями кибератак в этом сегменте становятся:

- финансовые потери;
- репутационный ущерб;
- штрафы за нарушение законодательства;
- судебные иски от пострадавших клиентов.

Ниже представлены примеры атак в сфере торговли, приводящие к реализации событий, которые влекут за собой негативные последствия для бизнеса.

Рисунок 2. Упрощенная схема кибератак на ретейл

К основным событиям, которые могут нанести бизнесу серьезный ущерб, следует отнести кражу любых данных и остановку продаж. Рассмотрим их детальнее.

Кража данных

В 2021 году, по нашей статистике, в 70% атак на компании из сферы торговли злоумышленники намеревались получить доступ к важной информации. В первую очередь хакеров интересовали персональные данные (32% от общего объема украденной информации), данные платежных карт (21%), базы данных клиентов (13%) и коммерческая тайна (13%). Чтобы их заполучить, злоумышленникам достаточно было взломать сайт либо получить доступ во внутреннюю сеть компании.

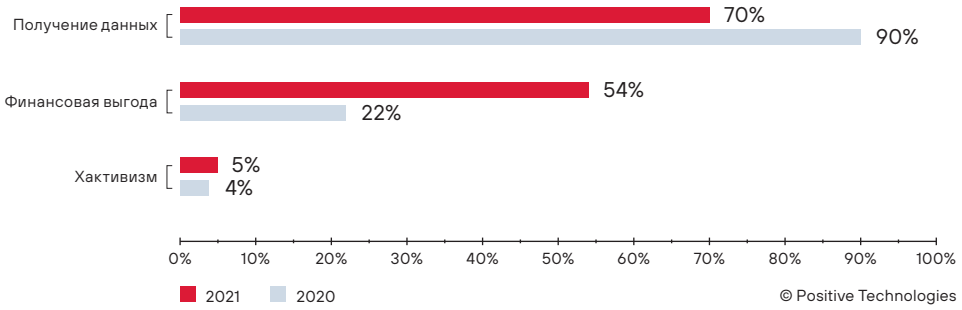

Рисунок 3. Мотивы атак на ретейл (доля атак)

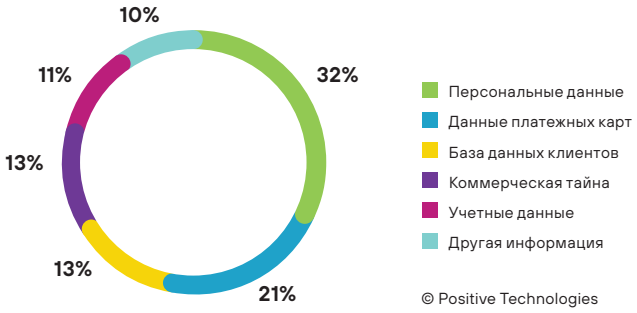

Рисунок 4. Типы украденных данных в атаках на ретейл в 2021 году

В нашем исследовании «Взлом на заказ» мы провели анализ объявлений на форумах в дарквебе, связанных с услугами по взлому сайтов, и выяснили, что примерно в семи из десяти запросов, касающихся взлома сайтов, основной целью было получение доступа к веб-ресурсу. Отметим, что хакеры могут не только похитить конфиденциальную информацию, но и продать доступ к веб-приложению так называемым скупщикам.

Рисунок 5. Распределение запросов в дарквебе по тематикам

Среди веб-ресурсов наибольший интерес для злоумышленников представляют именно онлайн-магазины: обусловлено это тем, что при оплате товаров пользователь указывает реквизиты банковской карты. В этом случае хакеру достаточно внедрить на сайт вредоносный код на языке JavaScript. Этот код будет перехватывать вводимую покупателем информацию, после чего злоумышленник может использовать полученные сведения в корыстных целях.

Пример атаки. Осенью 2020 года была зафиксирована атака более чем на 2000 интернет-магазинов, работающих под управлением CMS Magento. Злоумышленники использовали уязвимость 0-day для внедрения вредоносного кода на сайты и кражи банковских данных клиентов. Хакерская техника внедрения вредоносного JavaScript-кода на веб-страницы интернет-магазинов для хищения данных банковских карт получила название Magecart. Изначально так называли группировку, которая первой стала ее использовать. Техника оказалась настолько успешной, что вскоре у Magecart появилось множество подражателей.

Злоумышленник, получив привилегированный доступ к веб-приложению, может развить свою атаку до кражи баз данных и получения доступа к личным кабинетам пользователей. Используя сохраненные данные чужих банковских карт, хакер может оформлять заказы в интернет-магазине (или, воспользовавшись уязвимостями в приложении, вовсе не оплачивать товары). В дарквебе цены на доступы к интернет-магазинам варьируются в диапазоне от 50 до 2000 $.

Примеры атаки. В апреле 2021 года в дарквебе были выставлены на продажу 895 тыс. подарочных сертификатов общей стоимостью 38 млн $. База данных содержала сертификаты 3010 компаний, в их числе — Airbnb, Amazon, American Airlines, Chipotle, Dunkin' Donuts, Marriott, Nike, Subway, Target и Walmart. Предполагается, что злоумышленники получили к ним доступ в результате кибератаки на интернет-магазин подарочных карт Cardpool. Покупателю эти данные обошлись всего лишь в 20 тыс. $.

В марте 2022 года произошла утечка данных из сервиса Яндекс.Еда. В открытом доступе оказались данные более 6,8 млн человек: имена, номера телефонов и адреса. Позже в сети появилась интерактивная карта, на которой данные из Яндекс.Еды были объединены с утекшей информацией из Wildberries, CDEK, Delivery Club, ГИБДД и других источников. По адресу можно было найти номер телефона человека, дату и место рождения, паспортные данные, профили в социальных сетях, модель автомобиля и его госномер и иную персональную информацию.

Другой метод атак на ретейл заключается в получении доступа во внутреннюю сеть компании и в дальнейшем развитии вектора, например, до получения доступа к POS-терминалам или иным внутренним ресурсам, заражения устройств ВПО. По результатам исследований защищенности корпоративных информационных систем от внешних нарушителей в 2021 году было установлено, что в 100% компаний злоумышленник может проникнуть в локальную сеть и получить доступ ко внутренним сервисам и системам.

Пример атаки. Злоумышленники похитили данные 2 млн кредитных карт покупателей у южнокорейской компании E-Land Retail. Хакеры взломали корпоративные сети компании, получили доступ к POS-терминалам и установили на них вредоносное ПО Clop. В течение года преступники незаметно похищали данные кредитных карт покупателей. Украденных сведений было достаточно, чтобы клонировать карты и затем расплачиваться ими в магазинах. Что же касается E-Land Retail, то торговому гиганту пришлось временно закрыть почти половину своих магазинов, чтобы восстановиться после атаки.

Остановка продаж: причины и последствия

Следующая категория негативных последствий атак связана с недоступностью инфраструктуры: ретейлер лишится части прибыли, если хакеры атакуют сайт онлайн-магазина, ERP-систему, кассовое оборудование или другие системы, без которых продажи приостановятся. Вдобавок злоумышленники могут нарушить работу систем хранения и транспортировки товаров, что может привести, например, к порче продукции, если речь идет о продуктовом магазине. DDoS-атака или дефейс сайта, механизм которого не отличается от того же взлома, могут нарушить работу интернет-магазина, а атака шифровальщика может серьезно повлиять на доступность инфраструктуры. По итогам анализа киберугроз в 2021 году в 79% атак на ретейл с применением ВПО злоумышленники пользовались именно шифровальщиками.

Пример атаки. Весной 2021-го в Нидерландах шифровальщик попал в компьютерные сети поставщика услуг складского хранения и транспортировки Bakker Logistiek. В результате кибератаки все бизнес-процессы компании остановились: невозможно было ни получить заказ, ни определить, какие продукты и где именно находятся на складе, ни спланировать маршрут, чтобы отправить товар в магазины. Поскольку услугами Bakker Logistiek пользовались в основном супермаркеты, происшествие привело к острому дефициту продуктов, в особенности сыра, в крупнейшей нидерландской сети супермаркетов Albert Heijn.

Работа на опережение: минимизируйте возможные потери

Большинство угроз ИБ в ретейле связаны либо с атаками на покупателей, что приводит к утрате их доверия, либо с доступностью сервисов — как сайтов, так и инфраструктуры. Результат один: ретейлер несет убытки в виде недополученной прибыли, потери товара, издержек на восстановление работоспособности инфраструктуры и оплаты штрафов. При этом недопустимые события для отдельно взятой компании уникальны.

Для того чтобы заблаговременно принять меры по защите, необходимо определить те события, реализация которых приведет к недопустимым последствиям (например, недоступность сайта, кража банковских данных клиентов, мошенничество в интернет-магазине), и внимательно подойти к их верификации. Для этого мы рекомендуем использовать возможности киберполигона. Площадка позволяет проверить сценарии реализации неблагоприятных событий (с учетом связанных с ними бизнес-процессов и систем), определить критерии их реализации, оценить работу средств защиты и антифрод-систем, а затем спланировать меры и действия, необходимые для защиты от кибератак и минимизации их последствий.

ptsecurity.com
pr@ptsecurity.com