РБК+

ТЕМАТИЧЕСКОЕ ПРИЛОЖЕНИЕ К ЕЖЕДНЕВНОЙ ДЕЛОВОЙ ГАЗЕТЕ РБК

Среда, 29 декабря 2021 | № 203 (3492)

Информационные технологии

ТЕНДЕНЦИИ | **Что делает уязвимой предновогоднюю онлайн-торговлю**

Онлайн-ретейл сталкивается с сезонным увеличением числа кибермошенничеств. Компаниям приходится все больше вкладывать в комплексную защиту данных — как техническую, так и организационную.

Подарки от хакера

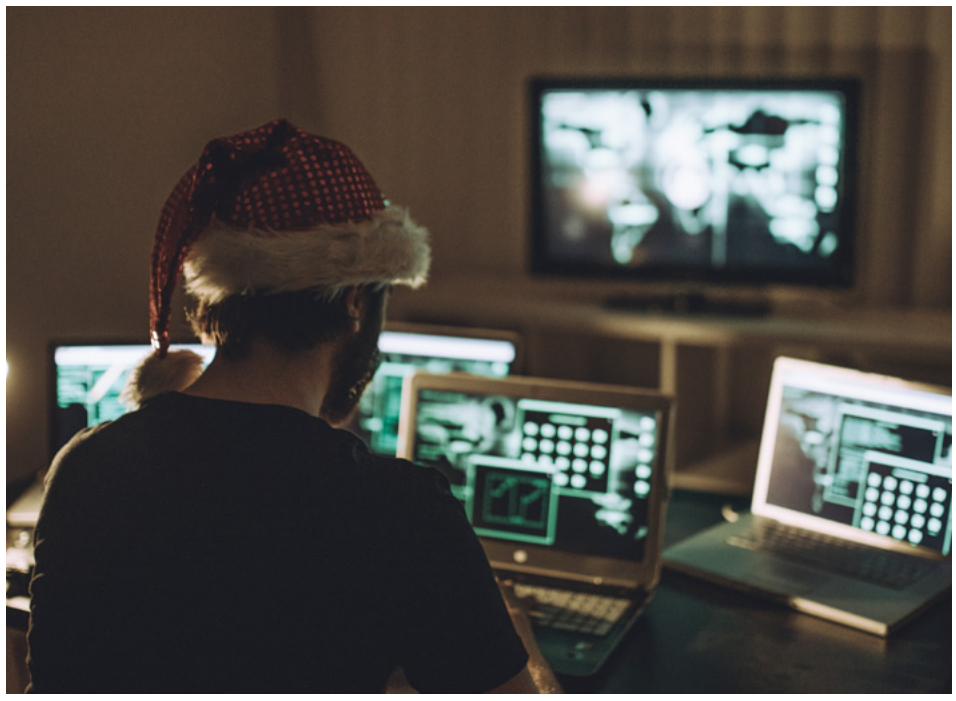

Фото: Getty Images Russia

МАРИЯ ПОПОВА

Пандемия и самоизоляция спровоцировали многократный рост кибермошенничеств на фоне повсеместной цифровизации и массового перехода на онлайн-платежи. По оценкам компании FreightWave, количество онлайн-преступлений в сфере e-commerce в мире увеличилось на 50% в 2020 году. Активность киберпреступников продолжает расти. По прогнозам исследовательской компании Juniper Research, убытки ретейлеров и площадок от мошенничества с онлайн-платежами превысят $206 млрд к 2025 году.

По данным компании «Информзащита», если в 2019 году объем операций, совершенных онлайн без согласия клиентов, составлял 6,4 млрд руб., то в 2020 году киберпреступники и телефонные аферисты заработали уже около 150 млрд руб. Из них 18,6 млрд руб. принесли фишинговые сайты и несуществующие интернет-магазины. В частности, в результате массовой атаки в сентябре 2021 года на интернет-магазин Wildberries потери составили до 350 млн руб., таковы данные «Информзащиты».

Традиционно всплеск мошенничества приходится на декабрь, в течение которого потребители чаще обращаются к электронной коммерции, отмечают в «Информзащите». В зоне риска — любой онлайн-бизнес, который работает с деньгами, а также с личными данными пользователей, включая их платежные реквизиты. «Нагрузка на сервис возрастает к концу года, в том числе связанная с кибератаками», — подтверждают в пресс-службе «СберМаркета». «Сезонность атак на онлайн-площадки ярко выражена», — согласен директор центра Solar appScreener компании «Ростелеком-Солар» Даниил Чернов.

Как правило, онлайн-платформы для розницы подключены к нескольким системам и партнерам, и если хоть одно звено в цепи будет сломано, скомпрометирована будет вся сеть. А различия в мерах безопасности на веб-сайтах продавцов создают условия для масштабируемых атак по побочным каналам. «Из-за растущего числа угроз информационной безопасности (ИБ) в розничной торговле отрасль будет становиться более подверженной утечкам данных и целевым продуманным кибератакам», — комментирует директор центра мониторинга, предупреждения и ликвидации последствий кибератак IZ:SOC компании «Информзащита» Иван Мелехин.

ЗОНЫ РИСКА

Самыми распространенными видами кибератак на онлайн-бизнес остаются фишинг, при котором мошенники создают фейковые сайты магазинов, платежных систем и т.д., чтобы получить деньги потребителей, и DDoS-атаки, когда злоумышленники одновременно отправляют множество запросов к серверу, чтобы вызвать сбой в работе онлайн-площадки.

В среднем в день появляется три—пять новых фишинговых сайтов. По данным компании «Информзащита», еще в сентябре интернет-мошенники совершили самую массированную атаку на клиентов ретейла в 2021 году. С начала месяца появились сотни сайтов, копирующих 15 брендов (включая «Дикси», «Ашан», «О'Кей», Wildberries, DNS, «Связной», «Ситилинк», Tele2, «Дочки-Сыночки», «Красное и белое», «Бристоль»), которые содержали опрос от имени ретейлера и розыгрыш денежного приза.

Число DDoS-атак на сервисы онлайн-ретейла по всему миру во время первой фазы пандемии (с февраля по октябрь 2020 года) увеличилось в четыре раза по сравнению с аналогичным периодом 2019-го, показало исследование компании StormWall. Самое большое их количество было направлено на онлайн-магазины по продаже техники (45%), одежды и обуви (32%), косметики (17%).

Также для атак на ретейл используются программы-вымогатели, которые с помощью шифрования закрывают доступ к корпоративной информации, а восстановить данные можно только после оплаты некоторой суммы или перевода биткоинов. Сохраняют актуальность и вирусы — вредоносное ПО, которое приходит в электронных письмах, например, с вложениями к поздравительным открыткам.

«Способов кражи логинов и паролей много, если пользователь пытался авторизоваться через фейковый вебсайт, при авторизации через публичные незащищенные Wi-Fi-сети, использовал комбинации из слитых баз данных», — поясняет Даниил Чернов. К примеру, при реализации сценария deface мошенники взламывают сайты и меняют одну или несколько страниц на официальном сайте. Пользователь кликает по ссылке, не понимая, что она создана злоумышленниками, и при оформлении заказа и проведении оплаты деньги получают мошенники. Похитив учетные данные пользователя сайта, они могут использовать в том числе и накопленные баллы программы лояльности, которые можно монетизировать в своих целях.

«Мошенники сейчас активно используют новые схемы, связанные с социальной инженерией, и мы постоянно отслеживаем мошеннические схемы, которые могут помешать пользователям делать заказы», — отмечают в пресс-службе «СберМаркета».

По данным «Информзащиты», почти 75% всех атак на онлайн-магазины совершается через отказ в обслуживании (DDoS), веб-приложения или скиммеры платежных карт. При этом отмечается рост профессиональной подготовленности мошенников,

«ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ» (18+)

Тематическое приложение к «Ежедневной деловой газете РБК»

Является неотъемлемой частью «Ежедневной деловой газеты РБК» № 203 (3492) от 29 декабря 2021 г.

Распространяется в составе газеты

Материалы подготовлены редакцией партнерских проектов РБК+

Партнер проекта: ПАО «Ростелеком». Реклама

Главный редактор партнерских проектов РБК+: Наталья Кулакова

Редактор РБК+ «Информационные технологии»: Владимир Новиков

Выпускающий редактор: Андрей Уткин

Дизайнеры: Дмитрий Иванов, Сергей Пивоваров

Фоторедактор: Алена Кондюрина

Корректоры: Татьяна Поленова, Маргарита Тарасенко

Директор по продажам РБК+: Евгения Карлина

их объединение в группировки (в том числе совместно с криминальными структурами) и значительные инвестиции в R&D (Research and Development — исследования и разработки) для улучшения своих инструментов.

МЕРЫ ЗАЩИТЫ

По оценкам «Информзащиты», в 2021 году компании розничной торговли уделяют приоритетное внимание кибербезопасности, стратегически планируя этапы по обеспечению комплексной безопасности инфраструктуры. Речь идет о защите персональных данных, а также процессинга, где происходят все платежи и операции по картам.

Сохраняется тенденция к увеличению бюджетов на информационную безопасность, а также к повышению уровня осведомленности персонала в вопросах ИБ. В частности, онлайн-площадкам нужно уделять внимание существующим уязвимостям, постоянно мониторить инфраструктуру, выявляя и анализируя инциденты, а также предотвращать утечки данных в частных облаках.

По данным «Информзащиты», в новом году компании, работающие с DevOps, будут обеспечивать безопасность своих приложений, внедряя технологии самотестирования, самодиагностики и самозащиты (пользуясь в том числе аутсорсинговыми услугами компаний по ИБ). Это поможет оценить новых поставщиков и обнаруживать возможные угрозы кибербезопасности в розничном ПО.

Чтобы онлайн-магазины могли противостоять атакам, которые совершаются непосредственно на них, необходима комплексная защита — сочетание технических и организационных мер безопасности, рассказывает Даниил Чернов. К примеру, онлайн-магазины могут отслеживать поддельные сайты-клоны и предупреждать покупателей либо с помощью email-рассылки, либо на сайте. А чтобы обезопасить их от несанкционированного списания бонусных баллов, следует ввести дополнительную верификацию покупателя после оформления заказа, добавляет эксперт.

Многие организации электронной коммерции не знают об уязвимостях своей ИТ-системы, пока не подвергаются первой атаке, комментирует Иван Мелехин: «И зачастую компании просто не осознают возможные масштабы ущерба из-за действий мошенников». Отчасти поэтому ретейлеры могут долгое время не обращаться к специалистам для разработки эффективной стратегии против фрода и кибератак. Но справиться со злоумышленниками в одиночку, по его мнению, сегодня не способна ни одна организация.

«Госуслуги» помогут бизнесу эффективнее взаимодействовать с гражданами»

Генеральный директор **ГК «РТЛАБС»** **ФАРИТ ХУСНОЯРОВ** — о том, чем цифровая экосистема «Госуслуг» может быть полезна бизнесу.

«Государственные цифровые платформы и сервисы дифференцированы. Сейчас основные сервисы для предпринимателей предоставляет ФНС РФ, а «Госуслуги» сосредоточены на оказании услуг для физических лиц. Наша с Минцифры задача — помочь бизнесу эффективнее взаимодействовать с гражданами, заложить в масштабах России фундамент соответствующей информационной экосистемы.

Сегодня есть 93 млн россиян — пользователей «Госуслуг» с полностью подтвержденными учетными записями. Об этих людях портал знает многое — дату рождения, паспортные данные, членов семьи, имущественный статус, получаемые доходы и т.д. Бизнес хочет получить доступ к этому массиву сведений, чтобы сделать путь до клиента максимально бесшовным.

Первое, что приходит на ум, — получение банковских кредитов или ипотеки. В 2021 году мы реализовали сервис, который позволяет банкам по согласию гражданина получать доступ к его верифицированным персональным данным на «Госуслугах». «Сбер» в этом году даже давал скидку 0,2% по ипотечным продуктам тем, кто воспользовался сервисом. Для самого банка такой подход сильно сокращает внутренние процедуры, связанные с проверкой заявителя, и банк этой экономией делится с самим клиентом.

К эксперименту по обмену данными Минцифры в скором времени хочет подключить и остальной бизнес. Разумеется, такой доступ предприниматели должны будут получать только с согласия пользователей.

В 2022 году мы хотим максимально внедрить новый проект — платформу подписания — мобильное приложение «Госключ». Сейчас, если возникает необходимость подписать какой-то договор, подавляющему числу людей все равно приходится ехать в офис банка, автодилера, риелтора, нотариуса и т.п. «Госключ» позволит подписывать любые бумаги дистанционно. «Госуслуги» фактически предоставят гражданину электронную цифровую подпись бесплатно, тогда как сегодня для получения персональной ЭЦП надо как минимум посетить удостоверяющий центр, заплатить несколько тысяч рублей, а через год продлить действие ключа. С «Госключом» для работы потребуется лишь учетная запись «Госуслуг» и личный мобильный телефон для СМС-авторизации.

Фото: пресс-служба

С помощью «Госключа» уже налажены сервисы дистанционной купли-продажи сим-карт. На упаковке практически каждой теперь есть инструкция, как скачать «Госключ», авторизоваться через «Госуслуги» и дистанционно подписать договор с оператором. Мы проводим тестирование аналогичных опций, например, позволяющих физическим лицам максимально упростить составление и подписание между собой договоров купли-продажи транспортных средств.

Много возможностей применения «Госключа» и в b2b-сфере. E-commerce, интернет-бизнес — агрегаторы услуг, ретейлеры, сервисы доставки постоянно и много взаимодействуют онлайн с другими участниками делового оборота. К примеру, у многих маркетплейсов есть собственная экосистема продавцов, с каждым из которых есть договорные отношения. Агрегаторы из сферы логистики взаимодействуют с курьерами, а курьеры — это микробизнес: они либо самозанятые, либо индивидуальные предприниматели, работающие с той или иной платформой. «Госключ» позволяет сделать так, чтобы все эти люди могли подписывать своими ЭЦП тысячи легальных договоров.

Обеспечение кибербезопасности «Госуслуг» для нас остается ключевой задачей. Более 90% атак связано не с недостатками защиты платформы, а с невнимательностью самих пользователей. Неслучайно уже в 2022 году будет введена обязательная двухфакторная авторизация на «Госуслугах»: помимо логина и пароля для входа потребуется СМС-подтверждение. Сейчас это добровольная опция, и мы благодарны тем сознательным гражданам, которые ею пользуются.

Защитой «Госуслуг» сегодня занята специальная структура «Ростелекома» — Центр кибербезопасности. Специалисты проводят мониторинг всех существующих хакерских сообществ, анализируют любую информацию, в том числе в Tor и DarkNet, которая касается возможных утечек данных «Госуслуг». Если некто в сети объявляет, что имеет украденный массив таких данных, Центр кибербезопасности делает тестовые закупки. На сегодняшний день не было ни одного подтвержденного взлома или утечки из «Госуслуг» персональной информации».

> Сегодня есть 93 млн россиян — пользователей «Госуслуг» с полностью подтвержденными учетными записями. Бизнес хочет получить доступ к этому массиву сведений, чтобы сделать путь до клиента максимально бесшовным»