07 августа 2019

Реальный кардинг: как сделать онлайн-платежи безопасными

Кардинг – это любые мошеннические операции, связанные с пластиковыми картами.

Какие виды кардинга существуют и как с ними бороться, рассказывает Сергей Прохоров, эксперт «КОРУС Консалтинг».

Потребители стали больше доверять онлайн-шопингу и активнее пользоваться пластиковыми картами. По данным Nielsen, 90% россиян совершили, по меньшей мере, одну покупку в интернете в течение последних двух лет.

Помимо очевидных преимуществ, использование банковских карт не защищено от определенных рисков не только для их держателей, но и для бизнеса, который может понести миллионные убытки и репутационные потери.

По данным ЦБ РФ, за 2018 год с карт россиян было похищено почти полтора миллиарда рублей. А глобальные потери, по данным Nielsen, составляют около одной десятой части процента от мирового оборота по пластиковым картам. При этом уровень тревожности держателей очень низок: люди не меняют пароли годами и продолжают пользоваться магазинами, которые

хранят данные их карт.

Существует несколько универсальных способов предупреждения мошенничества, при помощи которых бизнес может обезопасить транзакции своих потребителей. Однако важные аспекты безопасности и даже регуляторные требования по-прежнему часто остаются без внимания.

Каким бывает кардинг

Кардинг может быть двух типов:

- с физическим доступом к карте или банкомату,
- дистанционные атаки.

К наиболее очевидному мошенничеству относятся действия обслуживающего персонала, который может сканировать данные при помощи специального оборудования, изготавливать копию и снимать средства в банкомате. Но количество таких преступлений постепенно снижается.

Сегодня обслуживающий персонал приносит терминал к клиенту, а не уносит карту. На банкоматы ставят как физические средства защиты, так и электронные – для обнаружения скиммеров (миниатюрных устройств, которые крепятся к банкомату и считывают данные карт).

Кроме того, популярными становятся устройства с бесконтактными способами оплаты. Все это внесло вклад в сокращение случаев мошенничества со скиммерами.

Однако наиболее опасными до сих пор остаются атаки класса BlackBox, которые представляют собой подключение миниатюрного компьютера, заставляющего банкомат выдавать все деньги, что у него есть.

Международная ассоциация производителей банкоматов (ATMIA) в своем прошлогоднем отчете называла угрозу BlackBox одной из самых опасных, которая только начинает распространяться в США.

Эта атака стала возможной благодаря модифицированным утилитам производителей банкоматов, созданных для диагностики неисправностей. Ситуацию осложняет то, что производители считают потери от BlackBox менее значительными, чем расходы по перенастройке ПО банкоматов. Это приводит к тому, что современные банкоматы практически не защищены от угрозы BlackBox.

Самый популярный способ мошенничества, который сейчас и подразумевают под «кардингом», – это хищение данных с конечных устройств.

Переходя по ссылке, открывая неизвестное вложение в почте или вводя данные карты на неизвестном сайте, пренебрегающим защитой, пользователь рискует потерять данные.

Злоумышленник похищает всю информацию, относящуюся к банковским картам, криптовалюте, данные о системе, фото и видео, историю и настройки браузеров – то, что позволяет создать «цифрового двойника» жертвы. Все это нужно для того, чтобы кардер мог притвориться этим пользователем во время покупок.

Кто в зоне риска

В США онлайн-покупки уже давно стали распространенным явлением, а уровень обслуживания и удобства только растет.

Зайдя в интернет-магазин один раз, среднестатистический американец больше не хочет тратить время на поиск карты и желает, чтобы данные, которую он вводил ранее, заполнялись автоматически, а ему оставалось бы только нажать «оплатить».

И такое удобство, которого нет, к примеру, в России и Европе, онлайн-магазины обеспечивают несмотря на существование Payment Card Industry Data Security Standard (PCI-DSS) – стандарта безопасности, который не позволяет продавцу сохранять данные карт клиентов.

Интернет-магазин, который хочет сохранить покупателя, выбирает лояльного к требованиям PCI-DSS банка-эквайера. Кредитной организации тоже необходимо зарабатывать, и она разрешает сохранять данные карт, закрыв глаза на требования регулятора.

Для минимизации рисков потери данных банк, как правило, устанавливает антифрод-систему для оценки безопасности транзакций, интегрируя эквайринг в код интернет-магазина. Именно они и становятся жертвами хакеров.

Что при этом происходит после хищения данных клиентов? Ни интернет-магазин, ни банк-эквайер в США не будут афишировать взлом, поскольку это грозит штрафом от регулятора, потерей репутации и пристальным

вниманием со всех сторон.

Украденные данные продаются кардерам на черных рынках в даркнете. Для того чтобы примерить чужой «цифровой отпечаток» (операционная система, часовой пояс, язык системы, версия браузера), мошенники используют специальные системы антидетекта, находят прокси-сервер, наиболее близкий к дислокации владельца карты, и заходят через него в интернет-магазины и почту.

Там они предварительно «прогревают» карту, делая мелкие платежи, которые обычно совершал владелец, а спустя несколько дней выводят все средства, покупая дорогие товары на адрес владельца карты.

Затем подключаются местные преступники – «дропы», прекрасно владеющие языком, особенностями диалекта и спецификой разговора с магазином. Их задача – поменять чужой адрес доставки на свой и после получения товара переправить его или деньги (40-50% от стоимости товара) кардеру.

Интересно, что глобализация современной экономики позволила сделать кардинг очень доступным и масштабным во всем мире, помогая из разрозненных, узкоспециализированных преступных групп создавать практически бизнес полного цикла.

Уже прошло десять лет с момента атаки на Royal Bank of Scotland, когда злоумышленники сняли более девяти миллионов долларов с двух тысяч банкоматов в 280 городах по всему миру. Атака заняла менее 12 часов, после чего хакеры растворились, чтобы через год появиться на обложках таблоидов под реальными именами и не по собственной воле.

Крупные глобальные игроки, такие как Amazon, не хранят данные карт и вводят обязательное использование технологии защиты 3D Secure. Но и в этом случае найден workaround: у среднестатистического посетителя торговой платформы обычно имеется какое-то количество подарочных карт, которые не просят вводить номер карты и пароль.

Маркетплейсы знают про это: платежные системы получают свои роялти, интернет-магазины – деньги за товар, банки-эквайеры – процент за перевод. Стоит отметить, что среди крупных платежных систем есть и такие, которые жертвуют безопасностью ради удобства, как, например, PayPal – с привязанных к ней карт можно переводить средства без 3D-Secure.

«Серебряная пуля» и системы защиты

Чуть лучшим образом обстоят дела на российском рынке. По данным Fincert (структура ЦБ РФ, занимающаяся кибербезопасностью финансовой сферы), за семь месяцев 2018 года целевые атаки нанесли ущерб в 76,5 миллиона рублей вместо 1,08 миллиарда в те же месяцы 2017 года, несмотря на десятипроцентный прирост количества атак.

Многие отечественные компании защищены, но недостаточно. По разным источникам, 50-70% всех атак 2018 года были направлены на банковский сектор. Поэтому современной финансово-кредитной организации крайне важно иметь полное представление о происходящих процессах внутри компании.

Вот какие шаги необходимо предпринять для обеспечения безопасности:

- установка защитного программного обеспечения NGFW на всех точках входа и выхода в сеть для сегментирования и анализа трафика из/в ЦОД;
- контроль за движением файлов – большинство заражений происходит через почту;
- проведение ежегодного тестирования на проникновение и устранение найденных уязвимостей;
- регулярный внутренний аудит на выполнение распоряжений службы информационной безопасности;
- участие службы информационной безопасности в разработке мобильного приложения;
- создание прозрачного и неперегруженного процесса управления изменениями в ИТ и информационной безопасности;
- минимизация разрыва между выходом обновлений безопасности для информационных систем и их установкой;
- знание трафика, ходящего в сети и на периметре, протоколов и приложений, в рамках которых необходим обмен информацией;
- внедрение современных антифрод-систем на основе машинного обучения;
- максимальное вовлечение пользователей в процесс информационной безопасности: обучение, регулярные тренинги, разбор кейсов и инцидентов;
- изменение процессов продаж на новые, в которых кардинг невозможен;
- постоянный мониторинг черного рынка на предмет новых методов кардинга;
- и самое главное – выполнение всех требований регуляторов.

Хочется отдельно отметить, что безналичные платежи в России сейчас становятся все более безопасными. В нашей стране одной из первых появилась бесконтактная оплата устройствами, банки оснащаются современными средствами биометрической идентификации клиентов (в том числе и по голосу).

И важный момент: большинство кардеров боятся работать в России и СНГ, поскольку почти в 100% случаев их обнаруживают в течение короткого периода времени.

Источник: Rusbase