Аналитика и комментарии

Кросс-канальный антифрод – «серебряная пуля» для социальной инженерии

Издание: NBJ.ru, 29 декабря 2019 г.

Игорь Шульга, директор центра по противодействию мошенничеству «Информзащита»

Согласно отчету ФинЦерт Банка России за 2019 год, в 97% случаев мошенничества по отношению к физическим лицам использовались методы социальной инженерии: подмена номеров телефонов, переадресация вызовов, компрометация корпоративных электронных почтовых ящиков, кража личности (в том числе цифровой), др. Эту тенденцию также отмечают компании, работающие в области информационной безопасности и противодействия мошенничеству. Доклады каждой тематической конференции в РФ или на международной арене в течение года пестрят многочисленными фактами главенствующей роли социальной инженерии в мошенничествах.

Конечно, такие способы обмана фиксировались и раньше, но в меньшем количестве. Начиная с 3-4 кварталов 2018 года и далее в 2019 году этот способ мошенничества показал чуть ли не вертикальный рост, оказавшись большой проблемой для всей финансовой системы.

Что способствовало такому бурному развитию, и с какими задачами потребовалось справляться рынку для защиты своих клиентов и инфраструктуры? Прежде всего, совершенствование дистанционных каналов предоставления услуг клиентам, появление новых продуктов и сервисов увеличило поверхность атаки для мошенников. В то же время прогрессирует и адресное мошенничество с учетом информации об уязвимостях того или иного продукта и/или услуги. И это всё – наряду с ростом профессиональной подготовленности мошенников, их организованности в группировки (в том числе совместно с криминальными структурами и с распределенной юридической подотчетностью, что усложняет привлечение к ответственности), значительных инвестиций в R&D для улучшения своих инструментов и увеличения внутреннего мошенничества.

Это ни в коем случае не ставит под сомнение вопросы необходимости цифрового развития финансовой экосистемы, а только показывает острую потребность концентрации внимания финансовых институтов на этой проблеме и взвешенного подхода к вопросам внедрения своих продуктов, услуг и проектирования систем противодействия мошенничеству. Сегодня в большинстве случаев такие системы являются моноканальными, т.е. одна – для банковских карт, другая – для дистанционного банковского обслуживания физических лиц, третья – для выявления внутреннего мошенничества и так далее. Параллельно с ними существуют системы

информационной безопасности и сессионного антифрода, интеграция с сотовыми операторами. Систем много, и все они нужны и на своем месте, но проблема в том, что мошенники активно стали развивать и использовать кросс-канальные атаки.

Что такое кросс-канальные атаки? Очень просто для мошенников, но практически не решаемо для систем противодействия мошенничеству и систем информационной безопасности в их текущем исполнении. Атака может начаться со звонка в колл-центр банка с номера телефона клиента, продолжиться попыткой регистрации на себя приложения мобильного банка, затем последует звонок с номера телефона банка клиенту и попытки входа в кабинет интернет-банка (и даже, возможно, с устройства реального клиента), и только потом могут последовать операции с платежами и переводами. Да, возможно, во всех перечисленных выше системах эти попытки и будут зафиксированы, но они не будут связаны в одно мошенническое действие, происходящее в определенный отрезок времени по отношению к конкретному клиенту и/или устройству клиента. Таким образом, атака будет замечена только транзакционной системой противодействия мошенничеству.

Решения такого рода не идеальны и, даже при хороших аналитиках и настройках, будут пропускать мошеннические операции. Это может, кстати, происходить и не из-за несовершенности системы или непрофессионализма аналитика. Зачастую, проблема в бизнес-требованиях снижения нагрузки на сотрудников банка и на клиентов. В этом случае блокируются легальные операции – это так называемые False Positive срабатывания. Подобные сложности можно решить с использованием алгоритмов машинного обучения совместно с rule-based системой, но в настоящий момент эффективность таких действий невелика. И проблема не в слабости применяемых алгоритмов, а, скорее, в их выборе, настройках и, главное, количестве и качестве данных, которые подаются на вход такой «коробки». В этом случае, эффективность алгоритмов можно значительно повысить обогащением данных из других систем.

Напрашивается очевидное, но непростое, с точки зрения проектирования и процессов интеграции, решение – кросс-канальный мониторинг в единой системе противодействия мошенничеству, своеобразная «серебряная пуля» или попытка её отлить в борьбе с высокотехнологичным обманом. Можно считать это уровнем зрелости и ответственности финансового института, так как требует согласованного действия многих его подразделений, вендоров, интеграторов, способных работать не только в моменте, но и на долгие годы вперед, в едином архитектурном решении и его сопровождении по всем интегрируемым системам. Наш опыт работы по проектированию и внедрению систем противодействия мошенничеству за 2019 год показывает, что ведущие банки уже приступили к реализации таких систем.

Но не будем забывать, что работы только со стороны реализации технологических решений недостаточно, и нельзя оставлять клиентов без информационной поддержки. Нужно проводить работу по повышению осведомленности пользователей (awareness) с учетом особенностей различного возраста, образования, социализации и т.п. Это также актуально и для противодействия различным схемам внутреннего мошенничества и повышения готовности сотрудников банков противостоять методам социальной инженерии. Есть отличные курсы Учебного центра Информзащиты, например, «Противодействие корпоративному мошенничеству сотрудников компании». В этой связи стоит отметить активную работу ФинЦерт Банка России в повышении финансовой грамотности населения. Есть, конечно, и другие ресурсы, которые в течение года активно наполнялись по мере появления сценариев социальной инженерии и направлены на различные группы населения. Проблема только в том, что этот процесс должен быть более масштабным и проникающим буквально в повседневную жизнь, чтобы создать определенный образ в сознании людей, который поможет им противостоять различным методам социальной инженерии. Как пример, можно рассмотреть размещение коротких и понятных слоганов в общественном транспорте. Наша компания также активно работает в этом направлении, и отличным решением в уходящем году было партнерство с компанией «Антифишинг». Это решение позволяет внести большой вклад в защиту клиентов от методов социальной инженерии наряду с услугами нашего Центра противодействия мошенничеству по созданию процессов и систем противодействия мошенничеству, включая их кросс-канальный вариант.

В заключение все-таки хочется поставить мажорную ноту. Прошедшие конференции Antifraud Russia весной и в декабре 2019 года показывают, что банки, регулятор, сотовые операторы, вендоры и интеграторы отлично понимают тенденцию роста мошенничества, направленного на манипуляцию клиентами, и готовы активно предлагать и применять новые решения для снижения его уровня. Кто-то уже в пути реализации таких решений, остальным пожелаем активно включаться в процесс, конечно, вместе с нами…