Антифрод: широким фронтом

Мошенничество многообразно. Больше всего это явление распространено в банках, причем не только в каналах ДБО.

текст
Ивана Шестака,
менеджера компании DIS Group

В инцидентах, связанных с мошенничеством, помимо внешних злоумышленников, нередко участвуют сотрудники банка, использующие данные им полномочия в личных целях, — бухгалтеры, ИТ-персонал. Эти люди могут подкорректировать себе кредитный процент или вовсе перевести деньги на собственный счет, и такое происходит регулярно.

В ОЖИДАНИИ ЗАКОНА

По объемам денег, похищаемых в российских банках, из квартала в квартал прослеживается геометрическая прогрессия. Причина этого отчасти кроется в том, что воровать деньги у клиентов банка стало легко: для того чтобы успешно провести атаку, не требуется иметь высокую техническую квалификацию. Достаточно обладать средним уровнем подготовки, тем более что информация о механизмах проведения подобных атак находится в открытом доступе.

Закон 161-ФЗ «О национальной платежной системе» должен полностью вступить в силу в конце 2012 года. Некоторые его положения обязывают банки при определенных условиях возвращать клиентам украденные деньги. Надо признать, что крупные российские банки, хотя и с неохотой, но все же возвращают клиентам похищенные с их счетов средства. Правда, если клиент является юридическим лицом, вернуть похищенное сложнее: в этом случае банку придется расстаться с более крупной суммой, чем при краже у физических лиц. Но в перспективе, если деньги не будут возвращены клиенту, он, вероятнее всего, сменит банк. И вот тут уже последнему приходится решать, что накладнее — терять клиента или вернуть ему деньги.

В принципе, направления, по которым с мошенничеством можно эффективно бороться, уже выявлены. Во-первых, в России недостаточно сильная законодательная база для того, чтобы мошенников привлекать к суду. Во-вторых, улучшения требуют процессы повышения квалификации и организационной культуры как в банках, так и в отношении самих пользователей. В-третьих, свою эффективность доказали технические решения, внедрение которых позволяет вести мониторинг и расследование инцидентов, связанных с мошенничеством.

ВНЕДРЕНИЕ ТЕХНИЧЕСКИХ РЕШЕНИЙ

Обычно в период финансового кризиса положение усугубляется, а число проектов по внедрению антифрод-систем увеличивается. Криминогенная обстановка по киберпреступлениям в России не хуже и не лучше, чем в других странах. Мы работаем с западными клиентами, общаемся с зарубежными банками и регуляторами и видим, что объем мошенничества там тоже очень большой. На Западе работают группы мошенников, еще более квалифицированные чем в России.

В России основная масса мошенников пользуется, если можно так выразиться, базовыми и средними, не очень передовыми методами. Однако есть и преступные группы, которые целенаправленно применяют весьма продвинутые схемы. Но то, что мы видели на Западе, с точки зрения сложности типичных сценариев мошенничества, у нас встречается редко. Возможно, по этой причине нет и серьезных отечественных разработок систем фрод-мониторинга.

В 2008–2009 годах объем финансовых киберпреступлений в отношении банков начал бурно расти, и безопасность многих банковских учреждений была поставлена под вопрос. Примерно в этот же период, с 2009-го, в компании DIS Group начало развиваться направление, связанное с противодействием различного рода финансовым преступлениям, в том числе направление, связанное с внедрением систем фрод-мониторинга. Специалисты DIS Group проанализировали сложившуюся на тот момент ситуацию на рынке фрод-систем и остановили свой выбор на решении израильской компании NICE Actimize, актуальном для нашего рынка. Среди российских разработок представлены в основном базовые решения, функционал которых не всегда достаточен для решения задач, возникающих у банков.

ПРИНЦИПЫ АНТИФРОДА

Цель фрод-мониторинга в том, чтобы предотвратить мошенническую транзакцию. Для этого надо выявить и проанализировать транзакцию, определить, что ее совершает не клиент банка, а злоумышленник, и далее либо заблокировать, либо передать на ручной контроль уполномоченному сотруднику банка, который примет решение о проведение транзакции с возможным телефонным звонком-подтверждением клиенту.

Опыт показывает: для эффективного решения этих задач система

фрод-мониторинга должна иметь развитые аналитические механизмы, в том числе включающие анализ исторического поведения. Такая система обнаружит, например, что клиент обычно не работает на компьютере, с которого в данный момент осуществляется перевод, или снимает деньги в банкомате, которым он никогда не пользовался прежде. Если сумма платежа за разовую покупку у конкретного клиента в данный момент многократно превышает обычную для него величину или деньги переводятся на счет получателя, с которым раньше клиент не работал, то система, обладающая соответствующими аналитическими механизмами, сможет довольно точно оценить, является ли эта транзакция мошеннической.

Разработка таких развитых систем — весьма трудоемкий процесс, и качественный продукт невозможно создать за один год. Технологии мошенничества эволюционируют, поэтому и система фрод-мониторинга должна очень быстро адаптироваться, учитывая эти факторы.

Современные системы фрод-мониторинга эволюционируют от простых базовых проверок к полноценной скоринговой модели.

ОТ БАНКА К БАНКУ

При внедрении системы очень важно учитывать характер банка — ведь борьбу приходится вести на уровне рисков, присущих конкретному финансовому учреждению. В разных банках стоят одни и те же типовые системы. Но анализ статистики показывает, что в каждом случае риски уникальны. Есть, действительно, общие черты, но все-таки имеется и своя специфика применения мошеннических схем. Двух одинаковых банков с точки зрения фрода мы не видели.

В свою очередь, банки не ищут решения для внедрения: они хотят получить, по сути, готовую коробку, с лучшими мировыми практиками. Такой продукт нужно оптимизировать под конкретный банк и под те проблемы, с которыми он сталкивается. Задача, возникающая при внедрении системы фрод-мониторинга в конкретном банке, — понять, какие сценарии мошенничества для него характерны, и донастроить систему фрод-мониторинга с ее готовыми аналитическими моделями преступлений на те риски, которые типичны для данного банка или могут возникнуть в будущем.

Компания NICE Actimize, решения фрод-мониторинга которой мы внедряем в банковских учреждениях, имеет богатый международный опыт противодействия мошенничеству в кредитно-финансовых учреждениях. Примечательна эта система тем, что для ее внедрения нужно быть не только специалистом в ИТ и в области информационной безопасности, но и профессионалом в конкретной сфере банковского мошенничества. Обычно в решение этих задач со стороны компании, осуществляющей внедрение, вовлечены как эксперты в области фрода, так и ИТ-специалисты, которые знают, как грамотно работать с системой.

НА УРОВНЕ СТРАТЕГИИ

В России в стратегию банка редко закладывают борьбу с фродом: обычно какие-то действия в этом направлении предпринимают, когда мошенничество уже есть в банке либо когда начинаются скандалы и разборки. Дополнительным стимулом для внедрения подобных систем является прессинг регуляторов (ЦБР или ФСБ).

А на Западе подход немного иной. Там исходят из того, что проблема в банковском секторе есть, и вписывают ее решение в стратегию развития, то есть действия по фроду планируют заблаговременно. Причем идут широким фронтом, понимая, что мошенничество есть и в ДБО, и в карточном бизнесе, что есть внутреннее мошенничество, кредитное мошенничество: под эти сценарии банки вырабатывают свои планы развития.

На Западе системы фрод-мониторинга применяются в банках, страховых компаниях, финансовом секторе. Отдельный сегмент — здравоохранение, потому что его услуги все в большей степени начинаются оплачиваться в режиме онлайн. Эта же проблема актуальна для операторов связи, в госструктурах, в ЖКХ — везде, где совершаются платежи.

Фрод-мониторинг — это не единственное средство защиты. Лучше не рисковать и дополнительно применять средства защиты других классов — одноразовые пароли, ЭЦП и проч. Фрод-мониторинг — это один из элементов защиты банков, равно как и антивирусная система, ЭЦП и т. д.

Надо отдавать себе отчет в том, что эксплуатации подобных систем сопутствует большой объем рутинной работы — ведь все платежи с минимальной степенью подозрительности передаются на ручной контроль операторам. Но система фрод-мониторинга позволяет оптимизировать операционные затраты, которые банк инвестирует на борьбу с фродом, то есть сократить количество операционистов, аналитиков, которые рассматривают ежедневные платежи. В награду за внедрение систем антифрода банк получит снижение репутационных рисков и лояльность клиентов.

С точки зрения совершенствования методов борьбы с фродом стоит отметить, что уже есть банки, которые на текущем этапе развития полностью исключили проблему мошенничества. Если эта проблема еще стоит, в первую очередь можно порекомендовать сделать свою стратегию противодействия мошенничеству, после чего переходить к конкретным техническим средствам защиты. CIO

Современные системы фрод-мониторинга эволюционируют от простых базовых проверок к полноценной скоринговой модели, применяющейся для оценки риска