Алексей СИЗОВ

Реализация хищения сотрудником банка максимально приближена к стандартной операции, которая не вызовет подозрений. Выявление такого мошенничества связано с решением задач, не всегда традиционных для классических систем контроля или противодействия мошенничеству. Как построить схему детектирования внутренних хищений, в частности со «спящих» счетов? Как сформировать общий массив данных, пригодных для анализа? Что делать, когда модификация IT-систем не представляется возможной?

Как построить единую модель анализа клиентских операций для противодействия внутреннему мошенничеству?

Алексей СИЗОВ,
компания «Инфосистемы Джет», Центр информационной безопасности, руководитель направления противодействия мошенничеству

Крупная часть рисков мошенничества — это риски хищения со счетов клиентов при помощи различных атак на дистанционные сервисы: классическое удаленное управление, компрометация платежных реквизитов с использованием аппаратных устройств (скиммеров) или вредоносного ПО, социальная инженерия. Количество таких атак, озвучиваемое консалтинговыми компаниями, близко к истине, но вот объем потерь от них сильно занижается. Наиболее масштабные случаи, направленные на крупные юрлица или VIP-клиентов, редко предаются огласке.

2015 г. выявил иной пласт проблем — уязвимость банков к таргетированным атакам: за последние пару лет зафиксировано более 10 существенных атак, объемы потерь по которым исчисляются миллиардами рублей.

Однако есть еще один сегмент, которому уделено крайне мало внимания, — это внутреннее мошенничество. Как показывает статистика, схема хищений с привлечением сотрудников банка является наиболее эффективной: КПД такой атаки очень велик, а риски на стороне мошенников невелики. Внутреннее мошенничество «раскинуло свои сети» в большинстве банковских процессов: это и клас-

Как построить единую модель анализа клиентских операций для противодействия внутреннему мошенничеству?

сические операционные риски (хищения со «спящих» счетов, нелегитимный выпуск платежных инструментов (карт, доступов в ДБО) или присвоение таковых). Далее следуют схемы, направленные на выполнение планов: навязывание услуг, их оформление без ведома клиента, использование данных клиента для предоставления кредитных продуктов и т.д. Потом идут более «изящные» схемы, связанные с псевдодоверительным управлением средствами клиентов, операциями на валютном рынке или рынке ценных бумаг. Крупные факты хищений происходят именно в рамках казначейств, депозитариев, инвестиционных подразделений.

В последнее время важной проблемой многих банков является борьба со «сливом» конфиденциальной информации клиентов, связанным с конкурентной борьбой. Рынок перенасыщен, борьба за клиента и сохранение существующих клиентов становится сверхприоритетной задачей для любого банка.

Кроме этого, устойчивым трендом последних нескольких лет является усложнение атак на банковские процессы и IT-системы.

Не стоит забывать, что, кроме направления контроля хищений и злоупотреблений сотрудников, внутренний контроль обеспечивает выполнение требований регуляторов, среди которых наиболее значимым сейчас стало соответствие Федеральному закону от 07.08.2001 № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма».

Можно долго искать причины и говорить о соревновании меча и щита как о противодействии атакующей и защищающейся сторон, но на поверхности лежит простое наблюдение. При непрекращающемся развитии средств защиты и их востребованности рынком (исходя из финансовых показателей вендоров и интеграторов) тот факт, что это развитие не сокращает объема ни атак, ни самих потерь, говорит об отсутствии одного из звеньев в защитных или контрольных механизмах. Поиск решения данной проблемы и является одной из главных задач как подразделений безопасности в целом, так и подразделений внутреннего контроля в частности.

Создание единой структуры данных

Построение эффективных систем противодействия различным типам фрода и злоупотреблений сотрудников связано с решением задач, не всегда традиционных для классических систем контроля или противодействия мошенничеству.

Для построения единой модели анализа клиентских операций сквозь все каналы необходимо создать единую структуру из раз-

Алексей СИЗОВ

нородных данных. Она должна быть одновременно достаточной для выявления мошенничества. Сложность создания такого массива данных в том, что различные банковские системы отвечают различным требованиям к доступности данных, их резервированию и возможности предоставлять их третьим системам (например, антифроду). Создание единой схемы данных хотя бы с близкими показателями доступности — уже непростая задача. А сформировать и реализовать требования по достаточности данных: объему логирования, связанности сущностей в различных системах — задача более сложного уровня.

Необходимость такого большого массива данных для анализа также лежит на поверхности: реализация хищения сотрудником максимально приближена к нормальной операции, которая не вызовет подозрения, — сотрудник знает механизмы контроля и критерии отнесения такой операции к подозрительной классическими средствами. При этом первые и чаще всего ключевые действия сотрудников лежат вне стандартных операций: это может быть и поиск счета клиента с большим остатком без операций по счету (а операции read логируются крайне редко), и смена контактной информации.

Для построения единой модели анализа клиентских операций сквозь все каналы необходимо создать единую структуру из разнородных данных. Она должна быть одновременно достаточной для выявления мошенничества.

Получение таких данных из неподготовленных источников, из неструктурированной информации схем логирования и формирование общего массива данных, пригодных для анализа, — одна из важнейших задач для современной системы антифрода. Причем гибкость этой системы должна быть высокой: данные и источники, которые условно могут потребоваться для выявления схемы мошенничества завтра, нельзя определить сегодня. А значит, получение данных из таких источников должно отвечать требованиям простоты и оперативности.

В ряде случаев модификация IT-систем не представляется возможной, поэтому приходится прибегать к иным схемам получения сведений об активности в банковских приложениях (логированию, разбору трафика взаимодействия человека с системой или системы со своими компонентами). В нашей практике были случаи, когда для полноценной работы необходимых функций контроля использовались системы информационной безопасности SIEM, DAM, WAF. Они позволяли логировать действия без донастройки имеющихся источников данных или самостоятельно собирать информацию о действиях сотрудников.

Исходя из сказанного, схема детектирования хищения средств и нелегального закрытия вкладов по «спящим» счетам требует взаимодействия с АБС или бэк-офисным решением и предполагает

Как построить единую модель анализа клиентских операций для противодействия внутреннему мошенничеству?

поддержку возможности работы либо по API-интерфейсам, либо через корпоративную сервисную шину. При этом общие сведения по соседним системам, в том числе по действиям операционистов, требуют офлайн-работы с хранилищами и схемами хранения. А для получения данных о нефинансовых операциях, особенно о событиях просмотра карточек клиента, требуется работа с первичным логированием либо взаимодействие с ИБ-системами класса Database Application Firewall.

Логика выявления и анализа злоупотреблений

Следующей важной задачей является построение логики выявления и анализа злоупотреблений со сформированными данными. Есть нюансы и в части методологии анализа операций, а именно применимости подходов к контролю всех операций, исходя из контроля каналов. Подходы различны.

Использование rule-based подхода, правил по детектированию известных или ранее зафиксированных рисков является универсальным методом, но для выявления новой схемы мошенничества он не всегда результативен.

В то же время правила не имеют механизмов саморегулирования, что в свою очередь требует достаточного человеческого ресурса, который при необходимости может оперировать правилами анализа и изменять их. В случаях, когда происходит новая атака — массовые попытки совершения нелегитимных действий, скорость изменения логики становится ключевым параметром.

Примером такой атаки могут быть массовые попытки использования вредоносного ПО для компрометации среды совершения платежей и (или) подмены реквизитов. Если схема атаки сравнительно новая, то некрупные операции могут быть довольно успешными. При этом создать механику процесса контроля новой схемы, если она реализуется в вечернее время, крайне сложно ввиду отсутствия аналитиков и операторов разработки правил. Но математическая модель может быть обучена сведениями новых инцидентов, может начать выявлять расходные мошеннические операции сразу после обучения на первых потерях клиентов, которые необходимо просто зарегистрировать как инциденты силами оператора колл-центра банка, запустив обучение системы.

Поэтому возрастает потребность в актуализации моделей контроля процессов и поиске мошеннических или противоправных действий через анализ отклонений от стандартных показателей либо использование самообучаемых моделей.

Модели, основанные на механизмах машинного обучения, обеспечивают высокую скорость адаптации существующих сценариев к изменяющимся схемам атаки и естественным изменениям в работе клиентов, их количества и т.д.

Алексей СИЗОВ

Модели, основанные на механизмах машинного обучения, обеспечивают высокую скорость адаптации существующих сценариев к изменяющимся схемам атаки и естественным изменениям в работе клиентов, их количества и т.д. При этом роль специалистов, ответственных за эксплуатацию/настройку системы фрод-анализа, определяется уже не как роль разработчиков правил и политик (модель формируется и переобучается самостоятельно), а как роль контролирующего ресурса, подтверждающего качество работы модели, например параметров ложноположительных и ложноотрицательных срабатываний.

При этом в категориях и направлениях, где объемы мошенничества или сами факты довольно редки, применяются модели выявления аномалий поведения сотрудников, отклонения от бизнес-процессов.

Кроме того, антифрод-система обеспечивает взаимодействие между различными подразделениями безопасности, чья совместная работа гарантирует высокий результат, лояльность клиентов и создание единой базы знаний.

Итоговые рекомендации

Разнородность банковских систем и сложность бизнес-процессов приводят к необходимости построения сложной схемы анализа, которая обеспечивает повышение уровня защищенности банковской организации от мошенничества. При этом ключевые рекомендации по построению процесса контроля операционных рисков, связанных с мошенничеством или злоупотреблением, могут быть такие:

1. Повышение качества средств аутентификации пользователей на рабочих станциях: переход от парольной политики к двухфакторной аутентификации или биометрии.

2. Увеличение объема операций, подтверждаемых «второй рукой», другим сотрудником. При этом нужно строить схемы подтверждения, как можно более защищенные от возможности их компрометации одним сотрудником.

3. Развитие механизмов идентификации обслуживаемых клиентов.

4. Построение автоматизированного контроля соблюдения общих требований к банковским процессам, описанных средств идентификации и аутентификации на базе систем противодействия мошенничеству с организацией реагирования по факту нарушений вплоть до автоматизированных приостановок расходных операций.