ИСТОРИЯ УСПЕХА

Система по борьбе с мошенничеством в каналах ДБО «Банка Москвы»

ОАО «Банк Москвы» – один из крупнейших универсальных банков России, предоставляющий диверсифицированный спектр финансовых услуг юридическим и физическим лицам. Основным акционером Банка является Группа ВТБ (96, 88%).

В настоящее время «Банк Москвы» обслуживает более 120 тыс. корпоративных и свыше 9 млн частных клиентов. Среди клиентов – юридических лиц – крупнейшие отраслевые предприятия, предприятия среднего и малого бизнеса.

Система борьбы с мошенничеством в каналах дистанционного банковского обслуживания (ДБО) юридических лиц охватывает более 100 офисов банка. Ее внедрение позволило в 5 раз сократить операционные расходы бизнес-подразделений на выявление и противодействие мошенническим операциям. Это самообучаемая система, которая адаптируется к изменяющимся схемам мошенничества и в автоматическом режиме выявляет и блокирует более 99,79% высокорисковых транзакций. Количество транзакций, требующих дополнительного «ручного» анализа, уменьшилось в 5 раз.

Автоматизированная система борьбы с мошенничеством позволила освободить более 70% персонала, который участвовал в ручной верификации подозрительных операций – теперь эти сотрудники занимаются развитием бизнеса.

Система создана на базе решения RSA Adaptive Authentication – это одно из первых внедрений в России.

ЗАСЛОН ДЛЯ ФРОДА

«Объем финансовых потоков со стороны юридических лиц, проходящих через систему ДБО банка, в 2014 г. превысил 30 тыс. платежей в сутки. При этом в пиковые часы она обрабатывает более 100 транзакций в секунду, – рассказывает **Василий Окулесский, начальник управления информационной безопасности Департамента по обеспечению безопасности “Банка Москвы”**. *– При столь большом количестве операций, требующих контроля, их анализ должен проводиться в чрезвычайно сжатые сроки, а влияние человеческого фактора на его результат необходимо свести к минимуму. Все это, а также скорость, с которой мошенники изменяют способы своей деятельности, поставили для нас внедрение системы управления рисками, обладающей возможностями самообучения в реальном времени, в ряд задач, критически важных для бизнеса»*.

Специалисты компании «Инфосистемы Джет» провели анализ информационной инфраструктуры банка, задействованной в процессе выявления мошеннических операций, обследовали организационную структуру подразделений эксплуатации и контроля канала ДБО, данные финансовых операций и статистику по выявленным фактам мошеннических действий. На основании этого были сформированы функциональные и архитектурные требования к системе по борьбе с мошенничеством.

Банк Москвы

«В процессе внедрения система борьбы с мошенничеством была интегрирована в инфраструктуру банка и подключена к системам ДБО и АБС с полным сохранением показателей их надежности и производительности, – комментирует **Алексей Сизов, руководитель направления по борьбе с мошенничеством Центра информационной безопасности компании «Инфосистемы Джет»**. – *Поскольку необходимо было создать механизм онлайн-взаимодействия между системами борьбы с мошенничеством и ДБО, наши специалисты писали техническое задание, в том числе, и для разработчика системы ДБО. Мы настроили процессы обмена данными с системами ДБО и АБС об операциях банковского обслуживания и результатах их анализа. Система борьбы с мошенничеством получает данные о пользовательской среде выполнения операций (device fingerprints), учитывает особенности клиентской базы банка, организационной структуры, реализуемых схем мошенничества. Разработаны программные процедуры выявления мошеннических операций, а также организационные механизмы реагирования на них»*.

После комплексного нагрузочного тестирования система была запущена в опытную эксплуатацию.

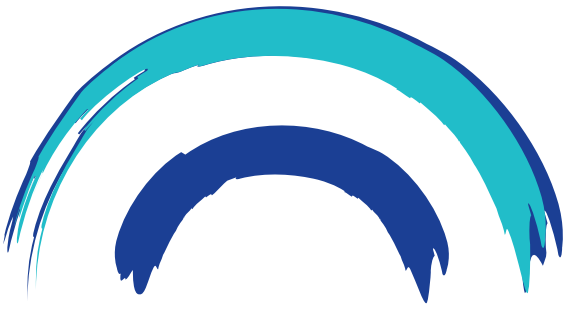
«Ключевой и наиболее ответственный этап проекта – обучение системы, – продолжает **Алексей Сизов**. – *В процессе опытной эксплуатации система борьбы с мошенничеством получает данные от продуктивных систем банка (данные должны быть реальными!) и строит математические модели для вероятностной оценки рискованности проводимых операций. В режиме обучения система не посылает сообщений в смежные системы, не блокирует и не приостанавливает никакие операции, только накапливает, запоминает и категоризирует события»*.

Продолжительность обучения системы составила около полугода. В этот период специалисты компании «Инфосистемы Джет» вручную помогали системе фиксировать типы событий, относящиеся к категории мошеннических. После запуска в промышленную эксплуатацию система полностью перешла на самообучение и самостоятельно совершенствует свою математическую модель. Сейчас «отлов» рисковых событий близок к 100%.

ТЕХНИЧЕСКИЕ ПОДРОБНОСТИ

Ядро системы борьбы с мошенничеством в каналах ДБО – RSA Risk Engine – в режиме реального времени оценивает онлайн-активность внешних пользователей, отслеживая свыше 100 индикаторов фактов мошенничества. Каждому действию присваивается уникальный балл риска в диапазоне от 0 до 1000 на основании байесовской модели, которая применяется для автоматической оценки вероятности риска по каждому индикатору. Окончательный балл риска складывается в результате комбинации баллов, зависящих от:

- недавнего поведения внешнего пользователя;
- данных, накопленных за длительный период;
- балла риска, назначаемого вручную (он используется для борьбы с новыми угрозами).



Василий Окулесский, начальник управления информационной безопасности Департамента по обеспечению безопасности «Банка Москвы»:

«Наш проект в некотором роде уникален – мы ставили своей целью не повышение уровня безопасности, а снижение стоимости самой процедуры выявления мошенничества. До этого 400 операционисток банка звонками подтверждали каждый новый платеж – их было около 10 тысяч в день. В результате проекта мы уменьшили количество контрольных звонков во фронтальных подразделениях при проведении платежей – по отдельным направлениям более чем в 10 раз. Нагрузка на операционисток снизилась, они переключились на продажу банковских продуктов – деятельность, напрямую приносящую прибыль».

За счет этого RSA Risk Engine борется с MiTM-атаками и троянами, реализующими атаки типа «Man-in-the-Browser». Байесовская аналитическая модель Risk Engine обнаруживает также новые, только формирующиеся схемы мошенничества, основываясь на анализе лишь небольшой части определенных операций. Вероятности в байесовской сети пересчитываются ежедневно, поэтому модель риска всегда является актуальной.

Возможности самообучения позволяют системе развиваться и адаптироваться для оперативного реагирования на любые изменения технологий, используемых мошенниками. Операции с максимальным баллом риска регистрируются в подсистеме Case Management, работающей в режиме реального времени. Информация о них немедленно возвращается в систему Risk Engine, и модель рисков обновляется.

Одним из элементов системы борьбы с мошенничеством в каналах ДБО является внешняя база данных RSA eFraudNetwork – межкорпоративная сеть, предназначенная для распространения и совместного использования информации о деятельности мошенников. Среди членов сети – десятки международных финансовых организаций, а также ряд ведущих мировых поставщиков интернет-услуг. Если атакам мошенников подвергся один из членов сообщества, все остальные немедленно получают об этом уведомления и защищаются от таких атак. Локальная копия базы данных eFraudNetwork, установленная в «Банке Москвы», обновляется каждые несколько минут, обеспечивая систему актуальными сведениями.

Благодаря перечисленным механизмам и функциям автоматизированная система борьбы с мошенничеством идентифицирует и блокирует рисковые транзакции «на лету», не создавая препятствий для работы в системе ДБО добропорядочных клиентов «Банка Москвы». Система эксплуатируется банком в промышленном режиме уже более года без снижения качества анализа и иных негативных факторов, влияющих на выявление мошенничества.

Россия, 127015, Москва
ул. Б. Новодмитровская, д. 14, стр. 1,
Тел.: +7 (495) 411-7601
Факс: +7 (495) 411-7602
E-mail: info@jet.msk.su
www.jet.msk.su