СВЯЗНОЙ БАНК

www.svyaznoybank.ru

ПРАКТИЧЕСКИЙ ОПЫТ СОЗДАНИЯ СОБСТВЕННОЙ АНТИФРОД СИСТЕМЫ

Начальник Управления
информационной безопасности
Департамента защиты активов
Лев Шумский

Собственная система ДБО

QBANK

СВЯЗНОЙ БАНК

TOP 10 INTERNET BANKING RANK 2014
Markswebb Rank & Report

synovate COMCON

GLOBAL FINANCIAL MARKET REVIEW

ФУНКЦИОНАЛЬНЫЙ И УДОБНЫЙ

Аналитическое агентство Markswebb Rank & Report присудило 4-е место интернет-банку QBank в России в 2014 году по результатам исследования Internet Banking Rank 2014.

ТОПОВОЕ МОБИЛЬНОЕ ПРИЛОЖЕНИЕ

Интернет-банк и мобильное приложение QBank вошли в ТОП-3 в категориях «Интернет-банк» (1-е место) и «Мобильный банк» (3-е место) на основе всероссийского независимого исследования компании Synovate Comcon.

ЛУЧШИЙ ИНТЕРНЕТ-БАНК 2014

Интернет-банк QBank признан лучшим в России в 2014 году по данным Global Financial Market Review.

Актуальные проблемы в ДБО

Кража реквизитов доступа

- Трояны на ПК/мобильных устройствах
- Социальная инженерия
- Замена сим-карты

Использование клиентами сервисов анонимного доступа

- прокси
- VPN
- TOR

Подходы к аутентификации

Классическая аутентификация.
Достаточно знания логина/пароля/OTP

Адаптивная аутентификация.
Анализируются дополнительные параметры и их изменения в динамике

Требования к антифрод системе

- Хотим всего и побольше…..

- Определение клиента по его поведению/«окружению» в момент аутентификации
- Возможность настройки и расширения функционала (например поведенческий анализ внутри системы, а не только процесса аутентификации)
- Как можно меньше денег на внедрение и поддержку ;)

Проблема выбора

Лидеры по Гартнеру

Отечественный производитель

Собственная разработка

Наш выбор

Собственное решение на базе Forge Rock OpenAM Adaptive risk authentication module

Основные этапы создания собственной антифрод системы

СВЯЗНОЙ БАНК

Разработка и утверждение ТЗ	3,5 месяца
Создание и тестирование модуля адаптивной аутентификации	3 недели
Сбор первоначальной статистики для обучения скоринговой модели	1,5 месяца
Обучение скоринговой модели	1,5 месяца
Проведение опытно-промышленной эксплуатации	3 месяца
Приемо-сдаточные испытания и перевод в промышленную эксплуатацию	2 недели
Итого	**~ 11 месяцев**

Выбор факторов адаптивной аутентификации

Изначально модель предполагала 5 факторов, сформировали дополнительно более 40

- Смена сим-карты
- Дата и время с момента последней успешной/не успешной аутентификации
- Расстояние с момента последней успешной/ не успешной аутентификации
- GEOIP
- IP Reputation
- …..

Дорогу одолеет идущий….

Включили логирование всех параметров и собрали нужный объем логов

В оффлайн режиме обучили модель

Оставили ТОП-20 наиболее значимых факторов, повторно обучили модель в оффлайне

Перевели на обучения в онлайн режиме, без принятия решения

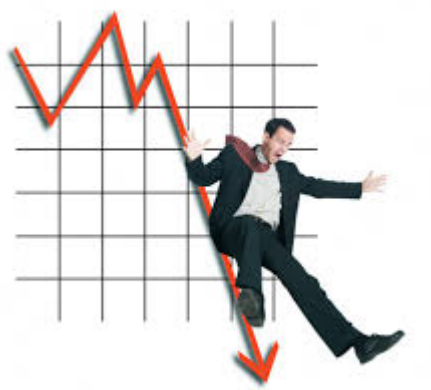
- Ложный отказ в доступе **8%**, качество модели **0,596**
- Ложный отказ в доступе **6%**
- Ложный отказ в доступе **2%**, качество модели **0,95**

Обучаем дальше

Нужен более длительный цикл обучения. Продолжаем опытно-промышленную эксплуатацию в пассивном режиме

Нужна проверка качества работы модели. Запускаем ручные процессы верификации предсказанного решения

А в это время в мире….

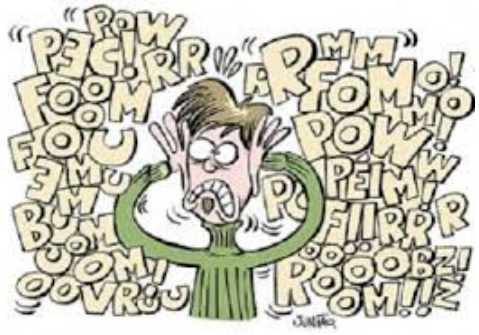


В связи с ситуацией на рынке вводятся лимиты на операции в ДБО

Транзакционная активность (в том числе и мошенническая) падает.

Промежуточные итоги

- Главное не количество факторов адаптивной аутентификации, а их качество. Избыточное количество факторов не улучшает результат, а дает шум.



- Нужно быть уверенным в достоверности значений получаемых факторов.

Выводы

Реализовать собственный антифрод

при наличии большого желания и небольшого бюджета

возможно!

Благодарю за внимание.

Вопросы?