

Jet Info

ИНФОРМАЦИОННЫЙ БЮЛЛЕТЕНЬ



ЗАЩИТА БАНКОВ ОТ МОШЕННИЧЕСТВА

№5 (????)/2012



ЕВГЕНИЙ АКИМОВ,
заместитель директора
Центра информационной безопасности
компании «Инфосистемы Джет»

На одном из последних круглых столов по ИБ, проводимых Национальным банковским журналом и Ассоциацией региональных банков, фактически единственной горячо обсуждаемой темой была проблема возрастающего числа случаев мошенничества в дистанционном банковском обслуживании и многомиллионных потерь от этого.

Актуальность этой тематики для банков многократно возросла после принятия Федерального закона № 161-ФЗ «О национальной платежной системе», регламентирующего возврат денежных средств при отказе от акцепта. Это означает, что с конца 2012 года банк несет не только репутационные и иные сложномонетизируемые риски в результате действий мошенников, но и риски финансовые.

Ряд банков уже успел начать пилотные и даже полноценные проекты по противодействию мошенничеству в ДБО, интерес же к этой тематике является весьма практическим для всех кредитно-финансовых организаций.

В этом номере Jet Info мы рассматриваем множество актуальных аспектов работы систем противодействия мошенничеству в ДБО: от общего понимания функциональности решения и последующего его распространения на другие каналы до факторов выбора технологической платформы и особенностей проведения пилотных проектов.

P.S. Нам важно Ваше мнение. Уделите нам минуту и оцените номер на сайте www.jetinfo.ru



12

**ЗАЩИТА ДБО:
ТРАДИЦИОННЫЕ
ПОДХОДЫ.**
АЛЕКСЕЙ ВОРОНЦОВ

17

**ЗАЩИТА ДБО
ОТ МОШЕННИЧЕСТВА
НА УРОВНЕ БИЗНЕС-
ПРОЦЕССОВ.**
АЛЕКСЕЙ СИЗОВ

24

**ЧТО НЕОБХОДИМО
УЧИТЫВАТЬ ПРИ
ВЫБОРЕ FRAUD
MANAGEMENT
SYSTEM.**
АЛЕКСЕЙ СИЗОВ

3

От редакции.
Евгений Акимов

5

Новости

8

Статистика

10

Во главе угла – защита
ДБО от мошенничества
Игорь Ляпунов

37

Наши проекты:
SS Мультикарта

40

В тему номера

28

**ПИЛОТИРОВАНИЕ FMS-
СИСТЕМЫ ДБО – ФАКТЫ
И ЦИФРЫ.**
АЛЕКСЕЙ СИЗОВ

30

**ЗАЩИТА СИСТЕМ
ДИСТАНЦИОННОГО
БАНКОВСКОГО
ОБСЛУЖИВАНИЯ
НА БАЗЕ РЕШЕНИЯ ORACLE
ADAPTIVE ACCESS MANAGER.**
АЛЕКСЕЙ СИЗОВ

33

**МОШЕННИКИ НЕ ПРОЙДУТ,
ИЛИ ВЫЯВЛЕНИЕ
МОШЕННИЧЕСТВА
С ПОМОЩЬЮ
RSATRANSACTION
MONITORING**



Электронная почта ВГТРК – под защитой



Всероссийская государственная телевизионная и радиовещательная компания (ВГТРК) и компания «Инфосистемы Джет» завершили проект по обеспечению безопасности электронной почты на базе продукта Proofpoint Enterprise Protection for Email Security. Построенная экспертами компании «Инфосистемы Джет» система защиты охватывает центральную площадку ВГТРК и 10 региональных. В совокупности это свыше 5000 пользователей. В дальнейшем планируется её масштабирование на все представительства телерадиокомпании.

ВГТРК – крупнейшая медиакорпорация России, имеющая более восьмидесяти региональных представительств на территории РФ. Специфика работы ВГТРК предполагает активное использование электронной почты для эффективной работы сотрудников и компании в целом. Поэтому ключевое значение для телерадиокомпании имеет задача обеспечения безопасности корпоративной почты, в том числе антивирусной защиты, спам-контроля входящего и исходящего почтового трафика.

Исполнителем проекта по защите корпоративной почты ВГТРК, благодаря глубокой экспертизе в сфере обеспечения безопасности электронных коммуникаций, стала компания «Инфосистемы Джет». Для защиты корпоративной почты ВГТРК, включающей две разнородные системы – Communicate Pro и MS Exchange 2010,

был выбран продукт Proofpoint. Он успешно решает проблему точной идентификации спама, используя сотни тысяч атрибутов для выявления нежелательных сообщений, и перемещает последние в карантин. Дополнительный модуль Proofpoint Zero-Hour Anti-Virus, входящий в состав внедренного продукта, опознает и блокирует новые компьютерные вирусы ещё до того, как для них выпущены сигнатуры. Облачная база репутации сообщений позволяет обеспечить эффективную защиту почты от спама без вмешательства в настройки системы даже при появлении новых видов спам-рассылок.

Проект длился 3 месяца. Проведенное на его первом этапе обследование выявило необходимость модернизации комплекса, выполняющего защиту и фильтрацию почтового трафика ВГТРК. Решая эту задачу, проектная команда развернула резервированное решение на двух серверах, на которых размещаются системы фильтрации вирусов и спама, система управления комплексом и карантин, позволяющий хранить нежелательные сообщения до трех недель. Оба сервера запускались в эксплуатацию поочередно, а общий поток входящих и исходящих сообщений разбивался на фрагменты и переводился на серверы поэтапно. Этот подход обеспечил непрерывность передачи почтового трафика во время проектных работ. Запуск каждого сервера сопровождался тестированием корректности его функционирования.

«Созданная специалистами «Инфосистемы Джет» система безопасности электронной почты в разы снизила риск возникновения атак, в том числе вирусных, и спам-рассылок, – комментирует Дмитрий Сафронов, начальник отдела защиты информации Дирекции информационных технологий ВГТРК. – Только за первые две недели своей работы система обработала порядка 10 млн сообщений, заблокировав 99% писем с неизвестными адресатами, содержащих спам, вирусы и иное вредоносное ПО. Это позволило нам повысить продуктивность работы своих сотрудников и значительно снизить репутационные риски компании, связанные с корректностью работы электронной почты».

«Помимо высокой результативности, разработанная система защиты электронной почты телерадиокомпании отличается простотой управления и требует минимального уровня вмешательства со стороны администраторов, – говорит Кирилл Викторов, заместитель директора по развитию бизнеса компании «Инфосистемы Джет». – А заранее заложенная возможность работы в облаке, которую предоставляет использованное нами решение Proofpoint, обеспечивает соответствие системы защиты концепции дальнейшего развития ИТ-инфраструктуры ВГТРК».

Облака становятся ближе

Компания «Инфосистемы Джет» получила специализацию IBM Cloud Computing (Cloud Builders) Specialty, что подтверждает высокий уровень экспертизы компании в сфере построения Private Cloud на платформе IBM. На сегодняшний день компания является единственным партнером в России и СНГ, получившим специализацию IBM по облачным вычислениям.

Специализация IBM Cloud Computing Specialty появилась в партнерской программе вендора в 2011 году и объединяет пять направлений: Cloud Application Providers, Cloud Builders, Cloud Infrastructure Providers, Cloud Services Solution Providers, Cloud Technology Providers. Компания «Инфосистемы Джет» получила специализацию по направлению Cloud Builders, что свидетельствует о компетенции системного интегратора в проектировании, построении и управлении частной облачной средой, а также в интеграции Private Cloud в инфраструктуру заказчика.

Для получения специализации сотрудники компании «Инфосистемы Джет» прошли обучение в IBM и успешно сдали экзамены, продемонстрировав глубокие знания не только облачных продуктов и технологий вендора, но также широкого спектра программных и аппаратных решений по другим направлениям.

Андрей Шапошников, заместитель начальника отдела проектирования вычислительных комплексов компании «Инфосистемы Джет» по развитию продуктов, комментирует: «Облачными вычислениями мы занимаемся практически с момента появления этой темы на российском рынке. В прошлом году совместно со специалистами IBM на территории IBM Innovation Center в Москве мы развернули первый в России облачный демо-стенд на базе ПО IBM Service Delivery Manager. Аналогичная пилотная зона открыта в московском офисе нашей компании для проведения тестирования облачных сред. Создание стендов, реализация пилотных проектов дали нам серьезный практический опыт автоматизации предоставления облачных сервисов, который мы готовы применить у наших заказчиков».

«Компания «Инфосистемы Джет» всегда уделяла большое внимание развитию технической экспертизы, что способствовало получению статуса IBM Cloud Builder. Продуктивное совместное сотрудничество даст возможность для освоения новых рынков и внедрения инновационных решений от IBM», – отмечает Евгений Кривошеев, руководитель отдела по работе с бизнес-партнерами, IBM в России и СНГ. 

«Инфосистемы Джет» – лидер по внедрению решений Blue Coat в России и странах СНГ

Компания «Инфосистемы Джет» продемонстрировала в 2011 году лучший результат по объемам продаж и количеству успешно завершенных проектов с использованием BlueCoat в России и странах СНГ. Доля компании «Инфосистемы Джет» в продаже технологий Blue Coat составляет более 20%.


Компания «Инфосистемы Джет» в третий раз становится лидером по внедрению и обслуживанию решений вендора. Так, в 2011 году было завершено более 20 проектов различной сложности с использованием технологий Blue Coat. В большей их части Blue Coat – основной элемент комплексного проекта, в состав которого также входят решения DLP.

Наиболее масштабными стали проекты по созданию систем управления и контроля доступа в интернет. Например, Банку «Санкт-Петербург» система контроля доступа в интернет предоставила широкие возможности для категоризации доступа к сайтам, защиты от вирусов, повысила эффективность работы сотрудников и качество предоставляемых клиентам сервисов.

В Банке Хоум Кредит построенная корпоративная система управления доступом в интернет позволила запускать новые интернет-услуги без расширения существующих каналов связи. Также в этом проекте были в полном объеме реализованы возможности решения Blue Coat для оптимизации трафика.

Крупнейшим внедрением решения Blue Coat на территории Украины стал проект в компании «Киевстар». Результат – создана максимально комфортная среда для работы сотрудников в глобальной сети Интернет. Система может быть использована и как платформа для предоставления новых абонентских услуг (родительский контроль, антивирус и др.).

«В прошедшем году мы отметили устойчивую тенденцию к росту популярности продуктов Blue Coat среди крупных игроков рынка. Более 30% реализованных нами проектов – внедрения в компаниях с большим числом пользователей и сложной ИТ-инфраструктурой. Это в два раза больше, чем, к примеру, в 2010 году. На сегодняшний день наиболее пристальный интерес к решениям Blue Coat проявляют компании с территориально-распределенными филиальными сетями», – резюмирует Кирилл Викторов, заместитель директора по развитию бизнеса компании «Инфосистемы Джет».

Партнерское соглашение между компаниями было заключено в 2007 году и позволило компании «Инфосистемы Джет» расширить линейку технологий, используемых в сфере web-безопасности и wap-оптимизации. 

Сертификату — быть

Уральский Банк Реконструкции и Развития совместно с компанией «Инфосистемы Джет» завершили комплексный проект по приведению платежных систем Банка в соответствие требованиям международного стандарта безопасности данных платежных карт PCI DSS 2.0. Проект затронул как платежные системы Банка, так и различные инфраструктурные системы, для которых был внедрен ряд необходимых средств защиты. После чего был проведен заключительный сертификационный аудит, завершившийся выдачей сертификата соответствия. При реализации проекта учитывались не только требования стандарта PCI DSS, но и другие актуальные потребности Банка в сфере обеспечения ИБ.

Уральский Банк Реконструкции и Развития – один из крупнейших отечественных банков, представленный в 19 регионах России. В числе услуг Банка значительную долю составляют те, в основе которых лежит использование пластиковых карт: оформление кредитных и дебетовых карт, корпоративных карт, зарплатных проектов и т.д. По количеству пластиковых карт, находящихся в обращении, Банк в прошедшем году вошел в двадцатку крупнейших в России. Объемы обрабатываемых в платежных системах данных делают обеспечение их безопасности, в том числе приведение платежных систем в соответствие требованиям стандарта PCI DSS, задачей первого уровня.

«Мы осознаем прямую взаимосвязь между надежностью Банка, доверием клиентов и общей его успешностью, – комментирует Александр Падерин, начальник управления безопасности информационных систем ОАО «УБРиР». – И проект по обеспечению соответствия наших платежных систем стандарту PCI DSS расценивается нами не толь-

ко как обязательная в финансовой сфере сертификация, но и как важнейшая составляющая ИБ Банка, поддерживающая уровень доверия к нам со стороны клиентов и партнеров на неизменно высоком уровне. Завершенный на сегодняшний день проект позволяет нам соответствовать ведущим тенденциям в области ИБ финансового сектора».

На первом этапе проекта были проведены обследование и оценка платежных систем Банка на соответствие требованиям стандарта PCI DSS, а также – уровня их защищенности в целом. По результатам данного обследования эксперты компании «Инфосистемы Джет» сформировали план мероприятий по приведению платежных систем Банка в соответствие требованиям стандарта, на основании которого в дальнейшем был разработан технический проект и внедрены необходимые средства защиты. В плане мероприятий по приведению в соответствие были учтены такие требования, как сохранение производительности информационных систем Банка при внедрении средств защиты и экономическая обоснованность используемых решений. В число впервые внедренных в Банке



средств защиты вошли:

- комплексное средство контроля целостности (Tripwire Enterprise);
- средство контроля доступа к сетевому оборудованию (Cisco ACS);
- средство мониторинга пользовательской активности баз данных (Imperva Secure Sphere);
- средства двухфакторной аутентификации.

«Каждый пункт плана приведения в соответствие и выполняемые работы мы детально прорабатывали вместе с ИТ- и ИБ-специалистами Банка, а каждое внедренное техническое решение предварительно тестировалось и настраивалось нами в соответствии с бизнес-требованиями Банка, – говорит Евгений Акимов, заместитель директора Центра информационной безопасности компании «Инфосистемы Джет». – Мы максимально задействовали уже имеющиеся в Банке технические средства защиты, использовали ранее средства защиты, встраивая их в инфраструктуру Банка таким образом, чтобы они не затрудняли работу Банка в целом, обеспечивали соответствие стандарту PCI DSS, а главное – имели практическую ценность для обеспечения реальной защиты информационных систем Банка. В частности, внедренные решения могут быть масштабированы в дальнейшем, в том числе с учетом требований российских регуляторов в сфере ИБ финансовых организаций».

Завершающим этапом проекта стал сертификационный аудит, который провели QSA-аудиторы компании «Инфосистемы Джет». Результаты аудита были представлены и приняты международными платежными системами Visa и MasterCard, после чего Банку был выдан сертификат соответствия требованиям стандарта PCI DSS 2.0. U

Завершен процесс создания нового вычислительного комплекса процессингового центра компании «МультиКарта»

Компания «МультиКарта», одна из крупнейших российских процессинговых компаний, и «Инфосистемы Джет», ведущий системный интегратор, завершили проект по созданию вычислительного комплекса для консолидированного процессингового центра.

Главной целью проекта было совершенствование ИТ-инфраструктуры «МультиКарты» в рамках программы модернизации процессингового центра (ПЦ) и повышения качества предоставляемых услуг.

Спроектировано и развернуто отказоустойчивое решение на двух зеркальных серверных площадках – в Санкт-Петербурге и Москве, благодаря которому удалось достичь максимальных показателей надежности и производительности вычислительного комплекса и как отдельно взятой серверной площадки, и как распределенного комплекса в целом.

В результате модернизации ПЦ расширились возможности поддержания растущих объемов бизнеса группы ВТБ и других клиентов компании «МультиКарта», существенно возрос потенциал для реализации востребованных технологических решений и предоставления клиентам качественных и удобных сервисов.

«Стабильный рост клиентской базы компании «МультиКарта» и увеличение нагрузки на вычислительные ресурсы потребовали обновления системы обслуживания процессинговых сервисов и, как следствие, создания для ее функционирования отказоустойчивого вычислительного комплекса, – говорит начальник управления вычислительных систем и телекоммуникаций компании «МультиКарта» Михаил Райнов. – Специалисты интегратора нашли для нас опти-

мальное решение с использованием самых передовых технологий консолидации и виртуализации вычислительных систем, благодаря чему наши планы были реализованы в полном объеме и без остановки сервисов».

«Стремительное развитие бизнеса часто диктует всё новые требования к бизнес-процессам. Во многом от того, насколько быстро эти требования выполняются, и зависит успешность всего предприятия, – резюмирует Андрей Шапошников, руководитель группы системной архитектуры компании «Инфосистемы Джет». – Над архитектурой решения мы работали совместно со специалистами заказчика, а также представителями разработчика ППО. С одной стороны, такое сотрудничество позволило нам более точно проработать конфигурацию и избежать многих ошибок на этапе проектирования комплекса, а с другой – мы наладили отличные партнерские отношения, что положительным образом сказалось на дальнейших этапах реализации проекта. В итоге комплекс был реализован в срок и отвечал всем предъявленным требованиям по надежности, производительности и масштабируемости».

Технические детали проекта

В рамках проекта спроектировано и развернуто отказоустойчивое решение на двух зеркальных серверных площадках – в Санкт-Петербурге и Москве. На базе комплекса установлено специальное прикладное ПО (ППО), которое обеспечивает синхронизацию данных, поступающих с самых разных сервисов группы ВТБ и других клиентов компании «МультиКарта».

Для создания вычислительного

комплекса используются вычислительная платформа компании IBM и дисковые СХД компании Hitachi Data Systems. Работоспособность баз данных для консолидированного процессингового центра обеспечивают четыре сервера IBM Power 570. Каждый сервер разбивается на виртуальные разделы с помощью встроенной подсистемы виртуализации IBM PowerVM. Данная технология используется для четкого разграничения и управления физическими ресурсами между виртуальными серверами, в каждом из которых работает одна из тестовых или продуктивных баз данных комплекса. Всего в комплексе задействовано свыше 90 БД.

Чтобы полностью исключить простой при плановом обслуживании серверного оборудования, а также для обеспечения возможности балансировки бизнес-нагрузки на серверы в режиме online в решении применяется технология Live Partition Mobility (входит в версию Enterprise продукта IBM PowerVM). Она позволяет переносить виртуальный раздел с одного физического сервера на другой цельным автономным сегментом, без прекращения работы бизнес-приложений.

Вычислительный комплекс был развернут на двух серверных площадках, находящихся территориально в Санкт-Петербурге и Москве. Площадки соединены между собой отказоустойчивым сетевым каналом связи. Оборудование на площадках полностью симметричное, конфигурация комплекса рассчитана на долговременную работу без потери функциональности и производительности основных информационных сервисов в случае полного выхода из строя одной из площадок. 

Новому ИТ-ландшафту – новая безопасность

Компания «Инфосистемы Джет» провела конференцию «Информационная безопасность нового ИТ-ландшафта: Virtual, Cloud & Mobile Security and Security for Business». Эксперты компании представили инновационные технологии по обеспечению ИБ и уникальные решения в сфере менеджмента её эффективности. Участниками семинара стали представители более 60 компаний, лидирующих в различных секторах рынка.

«До последнего времени развитие информационных технологий, таких как виртуализация, облачные сервисы, использование мобильных устройств, аутсорсинг, опережало решения по обеспечению их безопасности. Изменения, которые они привнесли в бизнес, столь значимы, что мы можем говорить о возникновении нового ИТ-ландшафта. Топ-менеджмент сегодня ожидает от такой специфической области, как ИБ, того же удобства, прозрачности и гибкости, которые предоставляют ИТ. Решения, которые мы рассмотрели, позволяют добиться большей эффективности и безопасности нового ИТ-ландшафта, – поясняет тематику конференции Евгений Акимов, заместитель директора Центра информационной безопасности компании "Инфосистемы Джет". – Кроме того, ИТ начинают применяться и для решения таких прикладных бизнес-задач, как противодействие мошенничеству и гарантирование расходов. Эти темы мы также не обошли вниманием во время семинара».

Пленарная часть мероприятия включила одиннадцать самых актуальных на сегодняшний день тем ИБ: безопасный аутсорсинг, контроль администраторов и аутсорсеров, инженерная инфраструктура интегрированных систем безопасности, использование Wi-Fi применительно к безопасности, системы класса Role Management, Fraud Management, мониторинг эффективности ИБ и др. Доклады спикеров основывались на практическом опыте компании «Инфосистемы Джет» по решению конкретных бизнес-задач с помощью технологий, большая часть которых появилась на рынке в течение прошедшего года.


На специализированных стендах, развернутых в демо-зоне, можно было познакомиться с решениями:

- по обеспечению безопасности мобильных устройств, базирующимся на Afaria и VDI;
- по защите виртуальных сред и облаков при помощи технологий TrendMicro и HyTrust;
- по управлению доступом на основе бизнес-ролей с использованием технологии Oracle Identity Analytics;
- по контролю ИТ-администраторов, основанными на Wallix и Spectr 360 на терминальной ферме;
- по мониторингу эффективности ИБ с использованием BI-системы QlikView;



- по контролю новых каналов утечки конфиденциальной информации на базе «Дозор-Джет» и др.

Темами для обсуждения на круглых столах стали такие сложные и неоднозначные вопросы, как совмещение требований бизнеса и российских регуляторов по ИБ в виртуальных средах, реализация требований стандарта PCI DSS на виртуальных инфраструктурах, защита ДБО от мошенничества и вопросы ИБ телекоммуникационных компаний. В качестве спикеров на круглых столах приняли участие ведущие специалисты компании «Инфосистемы Джет» и признанные эксперты отечественного рынка ИБ – Илья Трифаленков («Ростелеком») и Дмитрий Костров (МТС).

«Компании "Инфосистемы Джет" удалось в очередной раз показать свой высокий профессиональный уровень компетенции в области информационной безопасности, продемонстрировать комплексный подход к возникающим проблемам и представить нашему вниманию практически все современные тренды. Специалисты компании рассказали об апробированных решениях, продемонстрировали их на стендах. Наиболее интересными показались решения по безопасному использованию в бизнесе мобильных устройств и технологии VDI, а также материал по комплексному использованию Wi-Fi технологий для обеспечения коммуникации офиса и физической безопасности», – резюмирует Алексей Фролов, Руководитель Департамента по безопасности и режиму Корпорации «Иркут». 

Любимая игрушка хакеров



В отчете компании McAfee об угрозах за 3-й квартал 2011 г. констатируется, что ОС Android по-прежнему признается лидирующей на рынке мобильных устройств, и новые вредоносные программы пишутся в основном под нее. По сравнению с предыдущим кварталом количество вредоносных программ, написанных под Android, выросло почти на 37%. Это делает 2011 г. рекордным с точки зрения активности вредоносных программ не только на мобильных устройствах, но и в целом.

Аналитики G Data SecurityLabs считают, что скорость, с которой появляются новые вредоносные коды для Android, возрастает, в то время как небольшое количество обновлений для мобильной платформы шокирует. В 2012 г. аналитики прогнозируют еще большее распро-

странение вредоносного ПО для Android, причем эта платформа будет в какой-то степени напоминать Windows в том смысле, что «зловредов» станет еще больше, но это никак не повлияет на рост ее популярности среди пользователей.

Еще одним новым способом кражи информации клиента стало использование вредоносного ПО, которое записывает телефонные разговоры и пересылает их злоумышленникам. Примерами таких программ являются Android/Nicki Spy.A и Android/GoldenEagle.A. Злоумышленники обычно не ограничиваются прослушиванием одного-двух первых звонков, поэтому такая вредоносная программа может оставаться на устройстве продолжительное время, что делает ее очень серьезной постоянной угрозой безопасности. **||**

СТАТИСТИКА

СТАТИСТИКА

СТАТИСТИКА

СТАТИСТИКА

СТАТИСТИКА

СТАТИСТИКА

СТАТИСТИКА

И снова трояны

Как считают эксперты лаборатории G Data SecurityLabs, в прошедшем 2011 г. самым популярным способом вывода денег со счетов банковских клиентов было использование банковских троянских программ. По прогнозам аналитиков, в 2012 г. эта тенденция сохранится, так как количество пользователей онлайн-банкинга в России, как и во всем мире, постоянно увеличивается.

По разным оценкам, потери от онлайн-преступлений в нашей стране составляют порядка 500 млн руб. в год. По данным MForum Analytics, сейчас в России интернет-банкинг использует каждый десятый пользователь интернета. В 2012 г. этот показатель будет расти, в том числе и за счет увеличения числа людей, использующих онлайн-банкинг через мобильные телефоны. **||**



Год таргетированных атак

Как утверждают эксперты G Data SecurityLabs, в 2012 г. число таргетированных атак (так называемый целевой фишинг) и мобильных вирусов увеличится, в первую очередь вследствие того, что представители компаний и их незащищенные рабочие смартфоны являются особенно привлекательными жертвами для злоумышленников. Технологическая готовность последних такова, что они вполне могут получить не только корпоративную информацию с мобильных устройств, но и доступ в корпоративную сеть, например, если смартфон подключен к офисному Wi-Fi.

2012 г. станет годом таргетированных атак, предупреждают и специалисты McAfee. Реквизиты кредитных карт и банковских счетов с большим отрывом лидируют в списке информации, предлагаемой

к продаже на черных виртуальных рынках.

По данным последнего годового отчета компании Symantec, разброс оптовых цен на данные кредитных карт составляет от 17 долл. за 10 карт до 300 долл. за 1 тыс. карт. Для кражи этой ценной информации злоумышленники используют все доступные методы – от фишинга и спама до мобильных технологий. По данным Symantec, в 56% случаев фишинг-атак злоумышленники маскировались под банки. В целом же в ноябре 2011 г. объем спама на предприятиях финансовой отрасли составил 69,2%. Как считают эксперты компании, с ростом популярности мобильных устройств для совершения финансовых транзакций банки будут подвергаться все более сложным для определения угрозам.



СТАТИСТИКА

СТАТИСТИКА

СТАТИСТИКА

СТАТИСТИКА

СТАТИСТИКА

СТАТИСТИКА

СТАТИСТИКА

Мобильный банкинг идет в рост

Аналитическая компания Juniper Research подсчитала, что в 2011 г. число пользователей мобильных банковских операций достигло 300 млн. Наблюдая за развитием мирового рынка электронной коммерции, эксперты прогнозируют заметный подъем аудитории последователей мобильного банкинга – до 530 млн человек к 2013 г. Аналитики Juniper Research уверены, что популярность мобильного банкинга будет расти, несмотря на экономические проблемы в мире и угрозу усугубления глобальной рецессии. Более того, решения мобильного банкинга дадут банкам возможность повысить операционную эффективность и с наименьшими

затратами удержать и привлечь потребителя.

Согласно отчету Juniper Research, хотя финансовые учреждения уже разрабатывают собственные приложения для смартфонов и планшетов на базе iOS и Android, наибольший успех будут иметь запуски приложений с поддержкой «тройного экрана», SMS-сервисов и каналов предоставления услуг на базе браузера. Регионами-лидерами в области мобильного банкинга аналитики назвали Северную Америку, Западную Европу, государства Дальнего Востока и Китай, где наблюдается стабильный рост сервисов этих типов и ожидается самая высокая степень проникновения банковских мобильных сервисов к 2016 г.



ВО ГЛАВЕ УГЛА – ЗАЩИТА ДБО ОТ МОШЕННИЧЕСТВА



ИГОРЬ ЛЯПУНОВ,
директор Центра информаци-
онной безопасности компании
«Инфосистемы Джет»

«Правило ведения войны заключается в том, чтобы не полагаться на то, что противник не придет, а полагаться на то, с чем я могу его встретить; не полагаться на то, что он не нападет, а полагаться на то, что я сделаю нападение на себя невозможным для него».
Сунь Цзы, «Искусство войны»

Оборона всегда являлась следствием нападения и ответом на него. И ровно поэтому, говоря о средствах защиты от хакеров, нужно начинать именно со способов их атак и мотивации. Уже никто, к счастью, не вспоминает романтических хакеров начала девяностых, которые писали вирусы из «любви к искусству» и пытались доказать, что они тоже что-то могут и что-то значат. Им на смену уже давно пришел полноценный рынок, прагматичный расчет, баланс спроса и предложения.

Объем российского «черного» ИТ-рынка 3–4 года назад, по некоторым оценкам, составлял 200–300 млн долларов, в нем были задействованы несколько десятков тысяч хакеров с соответствующим разделением труда. Например, для одного из наиболее денежных сегментов – рынка спам-рассылок – «пищевая» цепочка выглядела следующим образом: одни вели исследования и писали эксплойты, другие запускали вирусы и собирали бот-сети, третьи продавали эти бот-сети, четвертые работали с «конечными заказчиками» и заряжали через них спам-рассылки.

Для еще одного фаворита – «пластикового» фрода (кардерства) – схемы были сложнее: одни добывали реквизиты банковских карт, например, в сговоре с кассовыми работниками «сферы обслуживания», другие изготавливали «белый пластик» или полноценные клоны карт, третьи их продавали, четвертые обналичивали.

За последние два года российский «черный» ИТ-рынок сильно изменился. И в первую очередь из-за смещения цели атак. На смену сложным, неочевидным и доста-

точно опасным схемам заработка пришли гораздо более прямые варианты – воровство денег с банковских счетов. Тем более что для этого уже всё есть: хакерские технологии, позволяющие извлекать любые конфиденциальные данные из компьютеров жертв, широкое распространение удобных систем дистанционного обслуживания в банках, привычка пользователей все делать через интернет. И как результат – миллиардные потери клиентов банков.

ТЕРЯЮТ КЛИЕНТЫ – ТЕРЯЕТ БАНК

Потери клиентов и банков в последнее время становятся все более тождественными.

Во-первых, проблемы с безопасностью при использовании сервиса ДБО приводят к серьезным репутационным потерям. Клиенты традиционно воспринимают банк как нечто надежное, в то же время при современном уровне распространения информации широко обсуждается практически каждый произошедший в этой сфере инцидент. Подобные факты могут стать очень неприятным сюрпризом для клиентов и суще-



ственно повлиять на выбор банка, которому будут отданы деньги на сохранение.

Во-вторых, в соответствии с законом № 161-ФЗ «О национальной платежной системе» в случае использования электронного средства платежа без согласия клиента (а под этим может подразумеваться совершение мошенничества третьими лицами) «оператор по переводу денежных средств обязан возместить клиенту сумму операции, совершенной без его согласия». При этом клиент не должен доказывать кредитно-финансовой организации тот факт, что «операция совершена без его согласия», — эта обязанность возлагается на банк. В итоге банки попадают в невыгодное положение: они обязаны нести расходы по возмещению, проведению расследования и судебные издержки. Кроме того, формулировки закона дают мошенникам дополнительную возможность для совершения преступных действий.

Еще одним моментом являются требования по контролю над рисками совершения мошенничества, которые выдвигаются международными платежными системами (МПС). Заключение договоров о присоединении к МПС и дальнейшая их реализация заставляют кредитно-финансовые организации постоянно демонстрировать факты исполнения этих обязательств.

Также в российском законодательстве прописана обязанность банка осуществлять мониторинг совершения платежных операций и определять факты совершения мошенничества со стороны клиента. Так, закон № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем» косвенно требует от кредитно-финансовой организации

создания системы, которая позволит в постоянном режиме отслеживать и устанавливать факты совершения мошеннических действий внутри своей клиентской базы.

ЧТО ДЕЛАТЬ

Для защиты систем дистанционного банковского обслуживания и, самое главное, клиентов банков необходимы усилия в следующих направлениях:

Обеспечение безопасности компьютеров клиентов банка: предъявление требований по обязательной установке средств антивирусной и сетевой защиты, установка обновлений, автоматический контроль выполнения этих требований, применение усиленных многофакторных средств аутентификации пользователей (токены, одноразовые пароли, виртуальные клавиатуры, скетч-карты), ЭЦП.

Обеспечение безопасности собственной инфраструктуры банка, защита публичных front-end серверов, каналов связи, установка средств обнаружения атак, средств контроля защищенности, систем мониторинга сетевых активностей и пр.

Активный мониторинг совершаемых транзакций, анализ их логики, контроль аномальных, не специфичных для данного клиента финансовых операций, времени и места их совершения, превышения лимитов по операциям, частоты транзакций, перевода денег на «подозрительные» счета и пр.

Повышение уровня осведомленности клиентов банка о том, что нужно, можно, а что категорически нельзя делать в интернете.

В последующих статьях каждый из этих способов будет подробно рассмотрен. ■

ДБО НЕ ОСТАНОВИТЬ

Сегодня одним из самых востребованных банковских сервисов является дистанционное банковское обслуживание (ДБО). Распространенность и практически неограниченный доступ пользователей из любой точки планеты, подключенной к интернету, обеспечивают ДБО преимущество перед стационарными сервисами. Благодаря мобильности и гибкости оно приносит банкам хорошую прибыль, а также увеличивает клиентскую базу, дает возможность оптимально реагировать на новые тенденции рынка, оперативно предоставлять другие сервисы и услуги. В настоящее время ДБО в России перестало быть термином, относящимся только к обслуживанию юридических лиц, хотя еще 5–7 лет назад это понятие прочно ассоциировалось со средним и крупным бизнесом. Тогда этот сервис предоставлял бизнесу возможность оперативно осуществлять распоряжения на совершение банковских операций. Сегодня системы ДБО для физических лиц стали неотъемлемой частью услуг любого банка, строящего бизнес на частных клиентах. И связано это со следующими факторами:

- развитием высокоскоростных сервисов оплаты услуг, которые больше не требуют от клиента посещения филиала банка или офиса компании;
 - конкурентной борьбой между банками и платежными системами виртуальных денег, которые первыми заняли сегмент осуществления операций через каналы массового обслуживания, в первую очередь, через интернет;
 - снижением себестоимости осуществления таких операций для банков (по некоторым оценкам – на 25–35%).
- Можно отметить, что развитая система ДБО для многих стала неотъемлемым критерием при выборе банка. Показательна и статистика: ежегодно на протяжении как минимум трех лет двукратно увеличивается объем операций на этом рынке.

ЗАЩИТА ДБО: ТРАДИЦИОННЫЕ ПОДХОДЫ



АЛЕКСЕЙ ВОРОНЦОВ,
архитектор инфраструктуры информационной безопасности компании «Инфосистемы Джет»



Защита клиентов дистанционного банковского обслуживания (ДБО) всегда была проблемой нетривиальной и потому интересной для профильных специалистов. И дело здесь не в защите систем ДБО банка, которая, по сути, ничем не отличается от обеспечения безопасности любого дистанционного доступа из недоверенной среды, имеет на вооружении целый ряд «лучших практик» и иногда даже попадает под действие регламентирующих стандартов, таких как СТО БР и PCI DSS. Нетривиальным остается одно — защита самих клиентских мест ДБО.

Компьютеры клиентов — это внешняя по отношению к системам банка территория, она не контролируется ИТ- и ИБ-службами банка. Организационные меры здесь в большинстве случаев не действуют — клиент всегда прав. Можно рекомендовать клиенту поставить на рабочее место, к примеру, антивирусное программное обеспечение, но реально работающих рычагов воздействия, гарантирующих выполнение этих рекомендаций, нет. Клиентские места при этом — самая массовая часть системы ДБО. И несмотря на то, что основной ущерб в случае нарушения ИБ на клиентском месте несёт именно пользователь системы, банкам тоже достаётся их «порция» — пока это только репутационные риски, миграция клиентской базы, участие в длительных расследованиях и разбирательствах. Однако ситуация может измениться в ближайшем будущем — с конца 2012 года, когда вступит в действие пресловутая статья 9 закона № ФЗ-161 «О Национальной платёжной системе» (она гласит, что если клиент уведомляет банк о неправомерном использовании

средств электронного платежа, банк обязан возместить ему сумму операции, совершённой без его согласия).

При этом число атак на клиентские места в последнее время всё возрастает. В этой сфере традиционно лидируют составители вредоносного ПО как способные на самую массовую атаку. По заявлению представителей МВД, в России за 2011 год один из наиболее частых видов киберпреступлений — это атаки именно на пользователей систем «Клиент-Банк». И при получении злоумышленниками того или иного вида доступа к счетам юридического лица ущерб в среднем составлял 3–5 млн рублей на организацию.

Наиболее распространённые способы атак на системы ДБО:

- вредоносное ПО (трояны, клиенты бот-сетей и т.д.);
- фишинг;
- использование атак типа Man-in-the-Middle для проведения подложных транзакций;
- внутренние атаки (для корпоративных клиентов);
- направленные атаки на клиентские места (опять же имеют смысл для корпоративных клиентов).

Соответственно, наиболее распространённые векторы атак на системы ДБО — это:

- хищение ключевой и/или аутентификационной информации с последующим ее использованием либо на месте, либо на удалённом компьютере;
- проведение транзакций непосредственно с компьютера клиента;
- подмена легитимных транзакций подложными.

С точки зрения возможностей защиты клиентские места ДБО можно разделить на два вида в

зависимости от специфики их применения. Первый — это защита традиционных решений «Клиент-Банк» (или «Банк-Клиент»), подразумевающих наличие «толстого» клиента и традиционно используемых при работе с юридическими лицами. Этот вариант предусматривает необходимость установки на рабочее место пользователя соответствующего пакета ПО.

Второй — это защита интернет-банкинга. В данном случае в качестве рабочего места пользователя выступает «тонкий» клиент, подразумевающий отсутствие какого-либо специализированного ПО на стороне клиента Банка. Этот вариант используется прежде всего при работе с физическими лицами, но приобретает всё большую популярность благодаря отсутствию необходимости устанавливать дополнительные программные и аппаратные средства, а также своей мобильности.

ЗАЩИТА СИСТЕМ «БАНК-КЛИЕНТ»

Как мы уже говорили, особенностью защиты «толстого» решения является наличие на рабочем месте клиента установленного комплекта ПО, состав которого определяет сам банк. То есть у кредитно-финансовой организации есть возможность выдвинуть ряд требований к программному обеспечению на конечной рабочей станции. Вводить в состав системы «Банк-Клиент» решение по endpoint-защите стало хорошей практикой в банковской среде. Из наиболее часто применяемых методов здесь — пассивный мониторинг активности в программной среде или даже комплексное решение, которое может включать в себя такие модули, как антивирусное ПО, хо-

стовый IPS, базовый персональный межсетевой экран, средства криптографической защиты информации (СКЗИ), возможность многофакторной аутентификации и т.д.

Что следует отметить, как хорошую практику использования традиционных средств защиты банк-клиентов? Список ниже:

Использование СКЗИ. Кроме применения криптосредств для защиты передачи информации по недоверенным каналам связи, хорошей практикой стало использование сертифицированных ФСБ СКЗИ для генерации электронных цифровых подписей (ЭЦП). Основная задача криптосредства в данном случае — обеспечение неотказуемости банковских операций в случае возникновения конфликтов (использование сертифицированных средств позволяет обеспечить юридическое основание при рассмотрении спорных случаев в судебных инстанциях).

Защита ключевой информации. Использование СКЗИ и ЭЦП для совершения банковских операций означает, что ключевая информация является в подобных системах «Клиент-Банк» одним из главных объектов атаки. Обладая этими данными, нарушитель сможет совершать легитимные финансовые транзакции от лица клиента. В связи с этим до-

полнительные меры для защиты ключевой информации всегда являются приоритетными. Среди основных тенденций — уход от применения накопителей и использование различных защищённых способов хранения информации, а также исключение ее хранения в недоверенной среде. Например, желательно использование процессорных смарт-карт и USB-токенов с возможностью совершения криптоопераций непосредственно на аппаратном устройстве.

Двухфакторная аутентификация. Дополнительным уровнем защиты может быть двухфакторная аутентификация сессии работы пользователей с системой «Клиент-Банк». Для этого можно использовать аппаратные и программные генераторы одноразовых паролей, токены и т.д.

Аутентификация на уровне транзакций. Проверка подлинности предполагает не единичную аутентификацию в рамках сессии работы системы «Банк-Клиент», а проверку при каждой из финансовых операций. Эта технология всегда способствует повышению уровня защищённости, но очень редко применяется для корпоративных клиентов. Дело в том, что при проведении большого количества платежей подобный режим вызывает слишком большое число нареканий со стороны самих пользователей системы.

Антивирусное ПО. Так или иначе, вредоносный код — это ос-

новной вектор атаки, в том числе и для корпоративных клиентов. Поэтому рекомендации по использованию комплексов антивирусной защиты на компьютерах с ДБО предлагаются практически всегда. Иногда в практике защиты встречаются случаи, когда антивирусная защита (хотя бы бесплатная) включается непосредственно в комплект поставки ПО «Клиент-Банк».

Использование комплексов Endpoint Security. Дополнительным уровнем защиты от внешнего воздействия систем «Клиент-Банк» является использование автономно управляемых (зачастую — с предустановленными рекомендованными настройками) комплексов Endpoint Security. Кроме антивирусной защиты, они могут включать в себя один или несколько компонентов: персональный межсетевой экран, хостовое средство обнаружения вторжения, средство криптографической защиты.

ЗАЩИТА WEB-БАНКИНГА

В случае web-банкинга всё богатство мер, традиционно используемых для защиты ДБО, оказывается в лучшем случае трудно применимым. Здесь преимущества web-технологий играют злую шутку. Отсутствие жёстких требований к программной платформе и устанавливаемого софта накладывает ограничения на защиту со стороны клиента. При этом риски для этой категории наиболее высоки. Что же традиционные средства защиты предлагают для web-банкинга? Список не

Компьютеры клиентов — это внешняя по отношению к системам банка территория, она не контролируется ИТ- и ИБ-службами банка



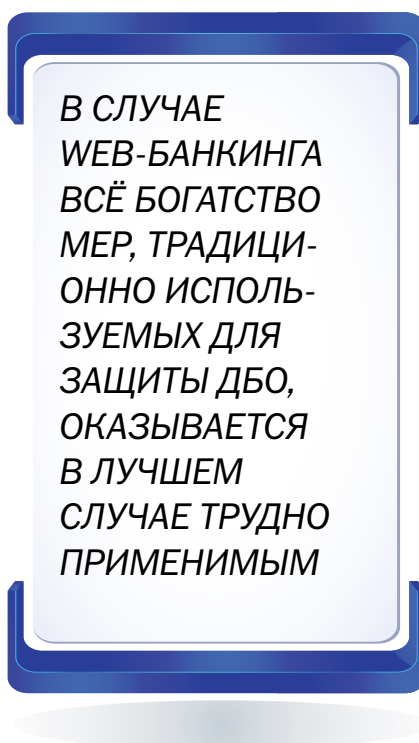
такой уж и большой:

Использование протокола SSL. Этот протокол позволяет обеспечить проверку подлинности сервера и шифрование сессии. Он применяется повсеместно в связи с тем, что реализован во всех современных браузерах, и позволяет избежать большого количества достаточно простых атак, таких как перехват аутентификационных данных или простые решения класса Man-in-the-Middle. В то же время протокол не обеспечивает защиту при компрометации браузера или подмене сертификатов корневых удостоверяющих центров на клиентских местах. Существуют также версии протокола с определенными слабостями и уязвимостями.

Защита от логирования данных доступа, которая подразумевает использование «виртуальных клавиатур», капч и других способов борьбы с перехватом и/или автоматизированным подбором аутентификационной информации. Увы, постоянное развитие вредоносного кода и различных систем логирования активности пользователя делает эти меры недостаточными. Однако их применение при построении систем web-банкинга не требует больших расходов и потому может рекомендоваться для использования.

Многофакторная аутентификация при доступе. Прежде всего используются решения с низкой стоимостью владения в пересчете на отдельного пользователя. Это блокноты с одноразовыми паролями, SMS-аутентификация или аутентификация с использованием ПО на мобильных устройствах (смартфонах, коммуникаторах, планшетах). Иногда возможно применение цифровых сертификатов на различных носителях, систем гене-

рации одноразовых паролей и даже биометрии. Но эти решения подразумевают высокие накладные расходы, как правило, лежащие на плечи клиентов при подключении к web-банкингу и потому применимы только в ограниченных случаях (к примеру, для VIP и имиджевых клиентов). Кроме того, некоторые из систем многофакторной аутентификации накладывают дополнительные ограничения



на используемые платформы, что может сводить на нет преимущества web-банкинга для клиентов.

В текущий момент наиболее популярным вариантом многофакторной аутентификации при доступе является именно SMS-аутентификация. Она предполагает достаточный уровень защиты при минимальных затратах и хорошо масштабируется (можно привести пример компании Google, использующей этот ме-

тод для доступа пользователей к сервису Gmail). Однако, по сообщениям McAfee Labs, новые версии вредоносного ПО уже научились компрометировать SMS-аутентификацию в ДБО путем реализации атаки Man-in-the-Middle прямо на коммуникаторе пользователя. Учитывая, что доля смартфонов и коммуникаторов растёт, а аудитория, активно использующая мобильные технологии, в достаточной степени совпадает с контингентом пользователей веб- и мобильного банкинга, число атак, реализуемых посредством компрометации смартфонов, будет только расти.

Аутентификация отдельных транзакций. Дополнительной мерой защиты может выступать использование многофакторной аутентификации не для получения доступа к системе web-банкинга, а для авторизации отдельных транзакций во время работы с ней. Способ обеспечивает частичную защиту от вредоносного ПО, работающего в уже открытой сессии пользователя. Для клиентов-физических лиц (в отличие от юридических) эта защита может считаться приемлемой ввиду удобства ее реализации: количество финансовых транзакций в рамках одной сессии в данном случае редко бывает значительным.

Оповещения о проведённых транзакциях. SMS и E-mail оповещения клиента о каждой транзакции могут также рассматриваться как средства борьбы с различными методами перехвата сессий работы с web-банкингом (хотя бы с точки зрения минимизации возможных потерь). Таким образом клиент всегда узнает о начале неправомерного использования его учётных данных. Кроме того, в соответствии с положениями нового закона

Хищение ключей ЭЦП

С момента развития защиты электронного документооборота, когда было сформировано понятие ЭЦП и приняты стандарты по его использованию, основным направлением атак злоумышленников стали попытки хищения ключей ЭЦП, расположенных на носителях разных типов. Такие хищения осуществлялись как самими сотрудниками компании, так и злоумышленниками с помощью взлома корпоративных сетей и персональных компьютеров, фишинга, внедрения вредоносных программ или социальной инженерии. Практика показала, что парольная политика защиты секретных компонент ключей не привела к значительному уменьшению атак, а лишь снизила вероятность использования ключа при прямой краже носителя. Хищения паролей ключей ЭЦП осуществляются аналогичными способами. Наиболее оптимальной защитой от подобных хищений стала практика хранения ключей на токенах – устройствах, исключающих копирование секретных данных и осуществляющих процесс подписи документа внутри токена. При этом факт хищения ключа легко распознается FMS-системами: признаками мошеннических действий являются получение платежного поручения с не зарегистрированных ранее компьютеров и IP-адресов, нарушение последовательности платежных документов или нестандартное для организации заполнение поля платежного поручения.



ФЗ-161, отсутствие уведомления клиента о совершённой транзакции рассматривается как безусловное перенесение ущерба от мошеннических операций на сторону банка.

Clientless NAC решения. В случае ДБО нельзя использовать полноценный In-Band NAC, поскольку отказ доступа к функционалу ДБО для пользователя с заражённого компьютера, даже реализованный из лучших побуждений, – это потенциально потерянный клиент. Однако предоставить информацию о наличии, к примеру, подозрительной вирусной активности со стороны клиентского компьютера или отсутствии антивирусного ПО никогда не бывает лишним. Ряд Clientless NAC-решений для контроля конечных рабочих мест работает напрямую из браузера и в случае обнаружения серьёзных уязвимостей позволяет выдавать клиенту предупреждение и список рекомендаций по дальнейшим действиям со ссылками на интернет-ресурсы. Другое применение подобных технологий – внутренний мониторинг клиентской базы с составлением списка подозрительных рабочих мест для последующей корреляции этой информации с данными систем финансового мониторинга и антифрода.

Clientless Endpoint защита. Это наиболее сложная технология, являющаяся развитием Clientless NAC решений. Фактически она представляет собой работающий в браузере (с использованием Java-апплетов, ActiveX и др.) полноценный endpoint-клиент, позволяющий без установки дополнительного ПО обеспечивать базовую защиту клиентских мест на время сессии работы с web-банкингом. Данное направление только развивается, практика использования подобных

решений очень невелика, однако их недостатки уже очевидны – это зависимость от версий ПО браузера и клиентских операционных систем, а также высокая стоимость владения.

Организационные меры, побуждающие клиентов к защите. Предложение клиентам ДБО льготных программ на покупку/аренду, к примеру, антивирусного ПО также может рассматриваться как одна из мер защиты клиентских рабочих мест.

ЗАКЛЮЧЕНИЕ

Количество угроз в сфере ДБО только растёт, и появляются новые типы атак, связанные с web-банкингом, вредоносным ПО для мобильных телефонов и др. Отметим, что некоторые из этих угроз еще не существовали год-два назад, с ростом рынка ДБО и банковских интернет-услуг растёт и привлекательность атак на данные услуги. Соответственно, растут потенциальные и реальные потери клиентов, а со следующего года – и реальные денежные потери банков.

При этом существует достаточно большой выбор средств и методов для защиты ДБО. Если говорить об их внедрении для массового использования, особенно для обслуживания физических лиц через средства web-банкинга, можно констатировать, что немногие решения проходят ценз стоимости и возможности масштабирования. В то же время сложившаяся на текущий момент ситуация с развитием киберпреступности и низкий процент раскрываемости подобных преступлений доказывают, что использование банками подобных технологий для защиты своих клиентов более чем оправдано. ▮

ЗАЩИТА ДБО ОТ МОШЕННИЧЕСТВА НА УРОВНЕ БИЗНЕС-ПРОЦЕССОВ

shutterstock

АЛЕКСЕЙ СИЗОВ,
архитектор FMRA решений Центра
информационной безопасности
компании «Инфосистемы Джет»

Наш опыт показывает, что противодействие мошенничеству в рамках дистанционного банковского обслуживания (ДБО), внедрение дополнительных и совершенствование существующих традиционных механизмов защиты не приводит к снижению рисков мошенничества до приемлемого уровня. Во-первых, это связано с тем, что усиление средств защиты побуждает мошенников разрабатывать все более изощренные средства атак, и этот процесс будет продолжаться, пока стоимость этих атак не приблизится к объемам похищаемых средств. Во-вторых, к сожалению, не все клиенты дистанционного банковского обслуживания контролируют общий уровень защищенности среды доступа к каналам ДБО.

Это заставляет кредитно-финансовые организации переносить некоторые меры контроля со стороны пользователя в свою зону ответственности. По мнению экспертов, новый рубеж защиты ДБО может быть эффективно выстроен на уровне бизнес-процессов, на котором осуществляется анализ логики финансовых операций. Любая совокупность данных об операциях клиента, информация о способе, месте совершения операции (т.е. точке доступа в систему ДБО) и адресате платежа является характеристикой пользователя. В общем виде набор этих параметров характеризует поведенческую модель. Используя статистические методы анализа, а также проводя постоянный мониторинг случаев совершения правонарушений операций, можно выстраивать системы, обеспечивающие предотвращение мошеннических действий. Более того, применяя обширный математический аппарат, можно осуществлять даже прогнозирование тех или иных событий.

ФУНКЦИОНАЛЬНАЯ АРХИТЕКТУРА СИСТЕМ FRAUD-МОНИТОРИНГА

Для выявления мошеннических действий оптимальной является глубокая интеллектуальная оценка банковских транзакций, которая становится возможной, если осуществлять анализ всего объема операций с помощью систем класса Fraud Management System – FMS (или систем Fraud-мониторинга, оба этих термина будут нами в дальнейшем использоваться). Эти системы позволяют осуществлять контроль всех банковских транзакций в системах ДБО в режиме online. Анализ того, является ли банковская транзакция мошеннической, проводится по предустановленным правилам, а также путем проверки соответствия логики действий клиента/организации его/ее профилю, который составляется заранее на основе исторических данных. По итогам такой оценки система Fraud-мониторинга позволяет предотвращать мошеннические атаки в соответствии с принятыми в банке процедурами реагирования на инциденты.

Эффективно задачу по анализу логики осуществляемых клиен-

том транзакций способны решить системы, которые имеют трехуровневую функциональную архитектуру, состоящую из:

- уровня интеграции, обеспечивающего сбор, обработку и нормализацию данных из тех источников, которые необходимы для осуществления анализа операций. Обработка данных и возвращение результата в ту или иную прикладную систему должны происходить в режиме online;
- уровня анализа данных, на котором происходят корреляция событий, профилирование клиентов, связывание различных категорий данных и, наконец, самое главное – обнаружение мошеннических действий с применением двух основных методик: на основе правил и с использованием поведенческих моделей;
- уровня представления данных, который автоматизирует управление решением вышеназванных задач, обеспечивает проведение расследований, реагирование на инциденты. Если в компании существует свой Workflow, то, как правило, процесс управления инцидентами мошенничества интегрируется с существующими в банке системами управления рисками.

Уровень интеграции:

сбор, первичная обработка и нормализация данных, возвращение результата анализа транзакций в интегрируемые системы

Уровень анализа данных:

корреляция событий, профилирование клиентов, связывание различных категорий данных, выявление мошеннических действий

Уровень представления данных:

представление результатов анализа, управление процессами, реагирование на инциденты, проведение расследований

Рис. 1. Функциональная архитектура системы Fraud-мониторинга



Подпись к рисунку вот таким образом. Не забудьте вставить настоящий текст Подпись к рисунку вот таким образом. Не забудьте вставить настоящий текст

Далее мы детально опишем каждый функциональный уровень.

Уровень интеграции

Для эффективной борьбы с мошенничеством в ДБО решение по Fraud-мониторингу интегрируется с информационными системами

банка, которые прямо или косвенно участвуют в процессе обработки удаленных транзакций клиентов. К ним могут относиться системы ДБО и АБС, а также другие подсистемы, с которыми FMS-решение может взаимодействовать для экспорта/импорта данных, необходимых при проведении анализа транзакций (серверы аутентификации и авторизации, web-серверы, базы данных, файловые хранилища и т.п.). Одна из возможных схем взаимодействия FMS-системы и информационных банковских систем изображена на рис. 2.

Интеграционная часть FMS-системы состоит из:

- подсистемы интеграции решения по Fraud-мониторингу и ДБО, обеспечивающей передачу данных о действиях и параметрах клиента. Эта информация накапливается в FMS-системе для анализа и построения профиля клиента;
- подсистемы интеграции FMS-решения и АБС, позволяющей системам взаимодействовать в процессе автоматического или ручного (выполняемого специалистом банка) анализа транзакций;
- подсистемы импорта данных справочников внешних систем, необходимых для нормальной работы

FMS-решения. Благодаря ей осуществляются консолидация и преобразование форматов представления;

- подсистемы экспорта результатов Fraud-анализа, обеспечивающей их выгрузку, преобразование форматов представления и подготовку к передаче во внешние системы.

FMS-решение может быть внедрено с использованием одного из нескольких поддерживаемых методов интеграции. Каждый метод предназначен для решения конкретных бизнес-задач и учитывает возможные технические и временные ограничения банка. Какие же существуют варианты?

Первый — это интеграция FMS-системы посредством ETL-инструментария (Extract, Transform, Load), обеспечивающего реализацию одного из основных процессов управления хранилищами данных. Этот процесс включает в себя извлечение данных из внешних источников, их нормализацию (для соответствия требованиям модели FMS-системы) и загрузку в хранилище данных (репозиторий).

Второй вариант — использование Web Services SOAP API, позволяющего строить взаимо-

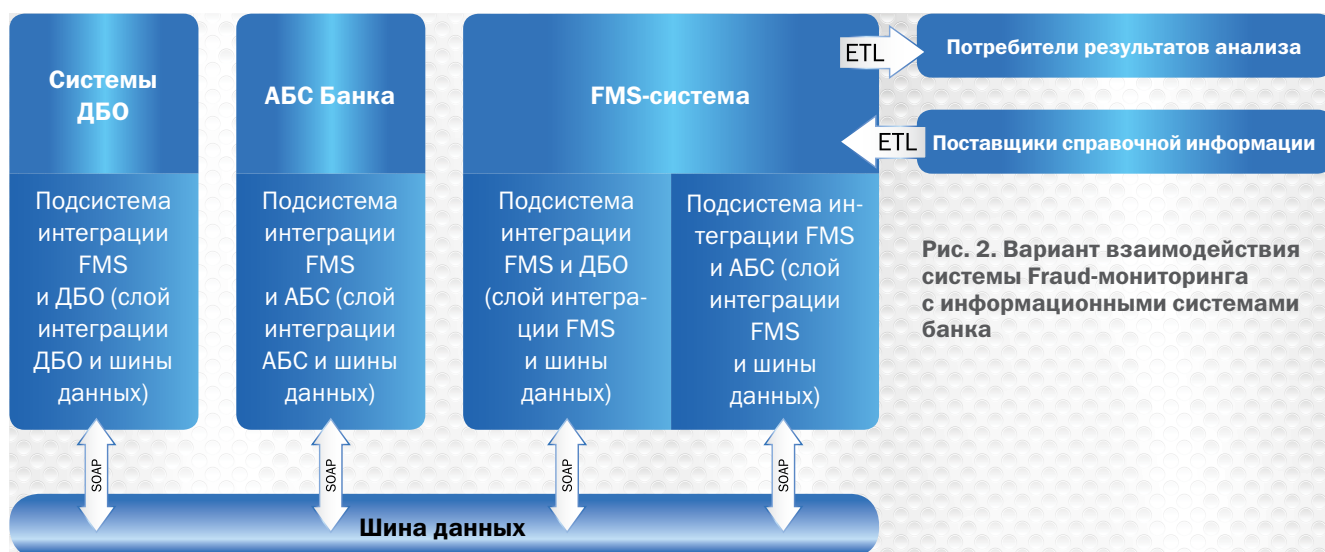


Рис. 2. Вариант взаимодействия системы Fraud-мониторинга с информационными системами банка

FMS-система анализирует платежные документы на соответствие построенной поведенческой модели, учитывающей, как минимум, следующие показатели:

- суммы платежей;
- получатели платежа (физические и юридические лица);
- назначение платежей;
- среднее/общее количество операций и их сумма за интервал времени;
- тип канала;
- IP/MAC-адреса и их география;
- идентификационный номер устройства (Device ID);
- используемые ресурсы (например, тип и наименование браузера);
- временной режим работы;
- «черный» список получателей;
- и т.п.

действие различных систем на уровне приложений, а не на уровне данных, как в первом случае. Благодаря синхронному режиму работы API такой вариант обеспечивает непрерывность процесса обработки операций, поступающих от системы ДБО, и позволяет передавать в бизнес-приложение результаты анализа по каждому вызову. Это наиболее широко применяемый метод интеграции, поскольку он дает возможность использовать преимущества всех функций FMS-системы в режиме реального времени.

Наряду с основными средствами многие разработчики ста-

раются добавить инструменты, которые призваны упростить механизмы интеграции. К таким инструментам относится, например, внедрение изображений размером 1x1 пиксель, которые размещаются на веб-странице сервиса ДБО. При этом информация из банковской online-системы собирается путем вызова изображения с сервера производителя FMS-системы. Этот вариант обеспечивает наиболее быстрое внедрение FMS-решения, поскольку не требуется разворачивание программных или аппаратных средств в Центре обработки данных банка.

Отметим, что сбор данных и возвращение результатов анализа в банковские информационные системы при работе решения по Fraud-мониторингу могут осуществляться в режиме как online (для текущих операций), так и offline (например, для загрузки исторических данных или использования полученных результатов сторонними потребителями).

Уровень анализа данных

Система Fraud-мониторинга осуществляет оценку операций на основании заданных правил выявления мошенничества. Анализироваться могут действия клиента, являющиеся как платежными, так и неплатежными операциями (запрос о состоянии счета, изменение своих данных и т.п.). Дополнительно в область действия FMS-системы могут попадать события, связанные со сменой сертификата доступа для дистанционного банковского обслуживания, с добавлением пользователей в ДБО или изменением их реквизитов, т.е. напрямую не относящиеся к операциям ДБО.

Критерием оценки при обработке операции в системе Fraud-мониторинга является результирующий скоринговый балл (показатель вероятно-

сти мошенничества), который сравнивается с определенными банком порогами значений для подозрительных операций. Каждое правило в процессе работы осуществляет проверку заложенной в него логической последовательности осуществляемых транзакций и изменяет оценку скоринга обрабатываемой операции.

В системе Fraud-мониторинга реализуются три класса правил:

- анализирующие выявления типовых признаков мошенничества. Создаются на основании экспертных оценок параметров рассматриваемой операции;
- осуществляющие анализ на основании профиля клиента, под которым понимается совокупность данных о совершенных им операциях, определяющая поведенческую модель. Любая новая транзакция может автоматически категорироваться относительно профиля клиента, что позволяет выявлять отклонения от поведенческой модели;
- выявляющие последовательность операций на основании данных о мошеннических схемах среди всего объема информации.

Рассмотрим общий алгоритм анализа операции системой Fraud-мониторинга. Для каждого клиента ДБО в процессе работы системы Fraud-мониторинга создается профиль пользователя, в который заносятся данные обо всех событиях по заранее определенным правилам. Профиль включает в себя такие данные, как:

- тип клиента (отправитель/получатель платежа, юридическое/физическое лицо, третье лицо/организация и т.п.);
- объемы и характер проводимых транзакций (большие/средние и мелкие платежи, время совершения операций и пр.);
- используемое оборудование/устройство (IP-адрес и т.п.) и территориальные признаки;

САМООБУЧАЕМОСТЬ FMS-СИСТЕМЫ – ВРЕЗКА

FMS-РЕШЕНИЕ ПОДДЕРЖИВАЕТ ВОЗМОЖНОСТЬ САМООБУЧЕНИЯ НА ОСНОВЕ ПОСТУПАЮЩИХ И НАКАПЛИВАЕМЫХ СВЕДЕНИЙ О КЛИЕНТАХ И РЕЗУЛЬТАТОВ АНАЛИЗА ОПЕРАЦИЙ. ПОД САМООБУЧЕНИЕМ ПОНИМАЕТСЯ АВТОМАТИЧЕСКАЯ НАСТРОЙКА ПАРАМЕТРОВ ОБЪЕКТОВ FMS-СИСТЕМЫ (СТРАТЕГИЙ, МОДЕЛЕЙ, СХЕМ, ПРАВИЛ, СЦЕНАРИЕВ И Т.Д.) С УЧЕТОМ ПОЛУЧАЕМЫХ ДАННЫХ.

В FMS-РЕШЕНИИ ПРЕДУСМОТРЕНА ВОЗМОЖНОСТЬ НАСТРАИВАНИЯ ПАРАМЕТРОВ ОБУЧЕНИЯ. СИСТЕМА УЧИТЫВАЕТ, ЧТО ПРИ АВТОМАТИЧЕСКОМ САМООБУЧЕНИИ МОЖЕТ ВОЗНИКНУТЬ СИТУАЦИЯ, КОГДА К РАЗРЯДУ ПОДОЗРИТЕЛЬНЫХ ИЛИ МОШЕННИЧЕСКИХ БУДЕТ ПРИЧИСЛЕНО СЛИШКОМ БОЛЬШОЕ ОТНОСИТЕЛЬНОЕ КОЛИЧЕСТВО (%) ПЛАТЕЖНЫХ ТРАНЗАКЦИЙ. СООТВЕТСТВЕННО, ПРЕДУСМОТРЕНА НАСТРОЙКА ПАРАМЕТРА, КОТОРЫЙ УСТАНАВЛИВАЕТ ОГРАНИЧЕНИЕ НА % ТАКИХ ОПЕРАЦИЙ. ТАКЖЕ ОРГАНИЗОВАНА НАСТРОЙКА ПОРогоВ СРАБАТЫВАНИЯ ПРАВИЛ, ОПРЕДЕЛЯЮЩИХ ПРИНАДЛЕЖНОСТЬ ОПЕРАЦИИ К МОШЕННИЧЕСКОЙ, ПУТЕМ ВЫЧИСЛЕНИЯ СКОРИНГОВОЙ ВЕЛИЧИНЫ.

- категория клиента (VIP, обычный пользователь и т.д.).

Кроме того, клиента в дальнейшем «связывают» с другими субъектами и объектами (финансовые организации, с которыми он взаимодействует, получатели/отправители платежей, его интернет- и сервис-провайдеры, другая необходимая для анализа информация). Далее FMS-системой формируются «белые» и «черные» списки, куда заносятся данные о параметрах совершае-

мых операций. Например, если ранее было зафиксировано более 3 транзакций с одного счета на другой и их данные были определены как легальные, то информация об отправителе и получателе заносится в «белый» список. В «черные» списки заносятся данные (IP- и MAC-адрес, имя пользователя, название компании, БИК и т.д.) о пользователях, ранее осуществлявших мошеннические операции.

В системах класса FMS любая транзакция первично проходит проверку на то, является ли она подлинной, инициирована ли она клиентом. Проверка осуществляется на основе анализа его действий, учитывающего отклонения поведения от ожидаемого. Если анализируемая транзакция не характерна для клиента, происходит количественная оценка вероятности (риска) того, что она может быть незаконной. Она осуществляется на основании заданных правил выявления признаков мошенничества или последовательности клиентских операций, эквивалентных существующей схеме мошенничества. Эти процессы осуществляются с помощью предустановленных или настраиваемых ключевых индикаторов, к которым могут относиться: дробление, округление (корректировка) счетов, открытие и закрытие счета в течение небольшого промежутка времени, всплеск активности по транзакциям, например, в ранее не фигурировавший банк получателя, перевод денег на счета в другие страны (если это не характерно для клиента), особенно из «черного» списка или в оффшоры, возобновление активности со «спящими» счетами и т.п.

В итоге для каждой входящей транзакции в соответствии с установленными правилами происходит вычисление параметра

скоринга, после чего ей присваивается соответствующее скоринговое число. Каждое правило имеет свой вес и коэффициент значимости, которые передаются в механизм подсчета рисков для принятия решения. Чем выше скоринговое число, тем больше вероятность (риск), что транзакция является мошеннической. В дальнейшем данные об операциях сохраняются в FMS-системе и могут быть запрошены при подсчете скорингового значения для других транзакций клиента.

В соответствии с предустановленными пороговыми значениями и на основании скорингового балла осуществляется передача результатов анализа в интерфейс обработки (данные становятся доступны для просмотра или принятия окончательного решения). Кроме этого, происходит формирование либо разрешения на проведение операции, либо события о запрете обработки. Дополнительно по итогам анализа могут быть активированы механизмы отправки уведомления о результатах подразделению банка/клиенту или команд во внешние системы для реализации дополнительного функционала (например, запуск процедуры дополнительной аутентификации).

Уровень представления данных

Автоматизированная обработка происходит за счет поддержки FMS-решением интеграции на уровне API или формирования команд для внешних систем. Критериями для ее осуществления могут служить специфические параметры операции в ДБО, показатель итогового скорингового балла или результат анализа любого правила выявления мошенничества. В свою очередь, командой может быть остановка обработки транзак-

ции, формирование уведомлений по каналу e-mail/SMS или запуск механизмов дополнительной авторизации совершения платежа.

В настройках системы Fraud-мониторинга реализуются следующие механизмы реакции:

- разрешение на выполнение транзакции или ее блокировка;
- задержка операции для осуществления дополнительных действий, например, передачи на анализ эксперту;
- внесение изменений в параметры обработки транзакций в информационных системах (АБС, Интернет-банкинг, процессинг и т.п.);
- оповещение уполномоченных лиц (экспертов, службы безопасности и т.п.) или передача принятия решения уполномоченному

специалисту банка;

- инициация дополнительной/повторной аутентификации;
- инициация дополнительного анализа данных по транзакции, субъектов и объектов, связанных с ней;
- или любая комбинация вышеперечисленных действий;
- блокировка/задержка транзакции и оповещение уполномоченных лиц;
- дополнительная аутентификация пользователей и в случае неудачи – блокировка транзакции и т.п.

Особое внимание необходимо уделить такому действию, как дополнительная аутентификация пользователей, поскольку оно образует еще один уровень обеспечения безопасности осуществления удаленного платежа.

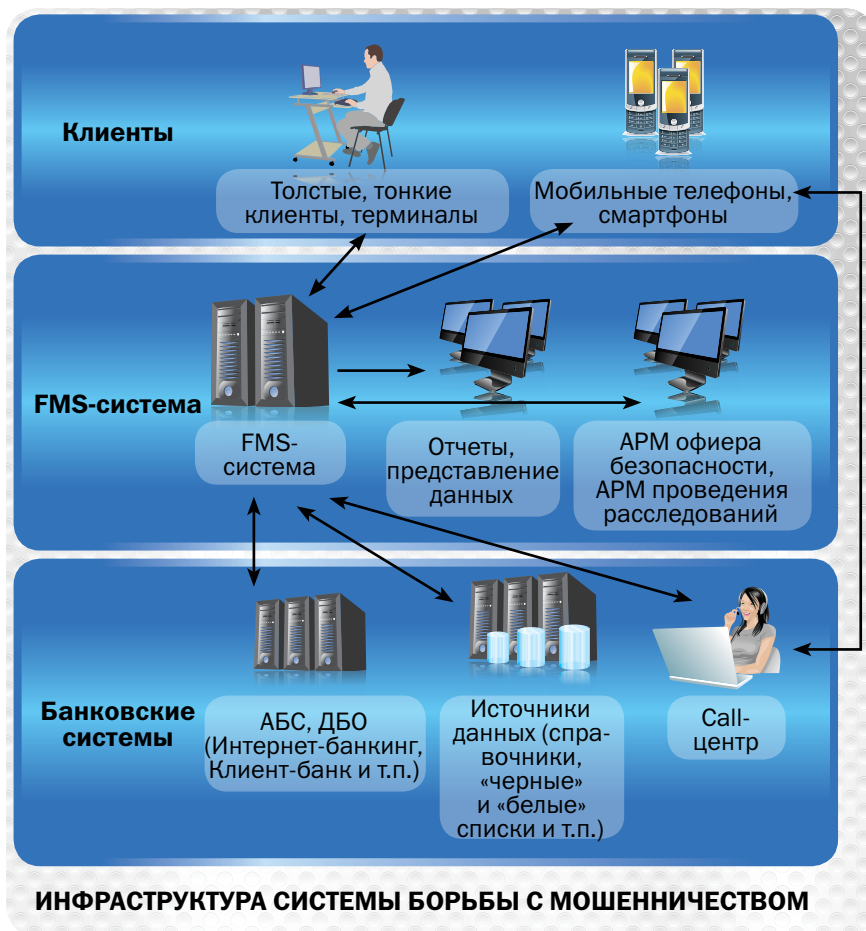
В случае если действие клиен-

та оценивается как подозрительное (например, вход пользователя осуществляется с нестандартного адреса), используется подсистема, которая автоматически предложит ему аутентифицироваться по более сложному алгоритму. Это может быть контрольный вопрос, который задается по телефону или по альтернативным каналам (SMS, e-mail, IVR, call-центр). Подсистема позволяет осуществлять аутентификацию по web-формам (Single Sign-On – SSO), одноразовым паролям, с использованием биометрии, смарт-карт, сертификатов X.509, а также идентификацию в каталогах и СУБД. Решение обеспечивает безопасность аутентификационной информации пользователей и защиту от действий таких вредоносных программ, как перехватчики данных с различных устройств (с клавиатуры – key loggers, с мыши – mouse loggers и т.п.).

Если после проведения автоматического Fraud-анализа система характеризует платеж как «подозрительный», ответственность за окончательное решение передается на ручную обработку уполномоченному сотруднику. Она реализована на базе web-интерфейса FMS-системы. Оператору доступен полный набор данных об операции, признанной подозрительной (исходная информация о транзакции, профиль клиента). При ручной обработке оператор принимает решение о правомерности совершаемой операции:

- разрешение обработки транзакции в АБС;
- отклонение обработки (документ/транзакция является мошеннической);
- запуск механизма дополнительной авторизации (в случае существования такой технологии).

Передача решения о разре-



шении/отклонении обработки операции ДБО в АБС банка может осуществляться с помощью API-интерфейсов и выполнения shell-команд (например, организации дополнительных полей в таблицах базы данных, интерпретирующих этап анализа транзакции FMS-системой и конечный результат). Для этой задачи могут быть как разработаны специализированные модули обработки передаваемых из системы ДБО в АБС транзакций, так и осуществлена доработка одного из решений (ДБО или АБС).

Система Fraud-мониторинга имеет в своем составе инструменты разделения прав доступа операторов к результатам анализа, что позволяет разграничивать работу с ней между территориальными подразделениями или группами обслуживания. С другой стороны, для нормального функционирования системы в подразделении достаточно иметь одно рабочее место Офицера безопасности на стороне FMS-решения.

Обработанные события канала ДБО могут быть наглядно представлены встроенными средствами визуализации системы Fraud-мониторинга. Среди таких инструментов выделяются:

- отчёты – Reports (компонент, предоставляющий исчерпывающую информацию о соответствии требованиям стандарта);
- активные каналы – Active Channels (компоненты для динамического отображения событий, поступающих в систему);
- мониторы данных – DataMonitors и DashBoards (графические панели для быстрой оценки ситуации);
- дела и расследования – Case Management (используются для организации Workflow-процессов, экспресс-проверок и проведения расследования).

АДМИНИСТРИРОВАНИЕ СИСТЕМЫ

Залогом построения эффективной системы Fraud-мониторинга является корректное построение модели выявления мошеннических действий. Для ее формализации в рамках FMS-решения организованы административные интерфейсы настройки, которые позволяют создавать, модифицировать правила выявления мошеннических операций, настраивать алгоритмы формирования профиля клиента, контролировать процессы обработки операций канала ДБО и детализировать результаты анализа. Современные системы позволяют управлять этими процессами через web-интерфейсы, при этом сам процесс настройки больше не сопряжен с необходимостью овладения языком программирования или внутренним метаязыком. Все административные действия осуществляются оконными интерфейсами, понятными пользователям бизнес-приложений.

ЗАКЛЮЧЕНИЕ

Таким образом, выстраивание «рубежа обороны» на уровне бизнес-процессов позволяет эффективно бороться с мошенническими операциями на стороне банка в том случае, если добиться соблюдения требований по безопасности на стороне клиента не представляется возможным. Как показывает наш опыт, именно системы Fraud-мониторинга, благодаря своей функциональности, способны обеспечить решение данной задачи. Трехуровневая архитектура таких систем является достаточно гибкой для интеграции в существующую банковскую инфраструктуру, при этом не возрастает нагрузка на ее производительность и не нарушается непрерывность бизнес-процессов. II

Удаленное управление

Совершенствование процессов защиты ключей для формирования ЭЦП привело к совершенствованию механизмов мошенничества. Ключ больше нельзя похитить из устройства хранения, однако осталась возможность его несанкционированного использования. Редкий клиент тут же вынимает токен после подписи документа, да и механизмы кражи паролей доступа к устройству – фишинг, трояны и спам-рассылки от имени банка – поразительно эффективны. Осуществляя взлом сетевой инфраструктуры предприятия путем кражи паролей доступов администраторов или все того же внедрения вредоносного ПО, злоумышленник получает доступ к компьютеру или с помощью специальных программ перехватывает управление. Клиенту демонстрируется страница «технических работ» на сервере ДБО, или просто имитируется «зависание» компьютера, а в это время злоумышленник осуществляет формирование мошеннических поручений и отправляет их в банк. Обнаружение этих атак основывается на выявлении отклонений от нормального характера платежных операций клиента, а также на совершении административных действий по смене паролей доступа к сервису ДБО непосредственно после отправки платежных поручений.





ЧТО НЕОБХОДИМО УЧИТЫВАТЬ ПРИ ВЫБОРЕ FRAUD MANAGEMENT SYSTEM



АЛЕКСЕЙ СИЗОВ,
архитектор FMRA решений Центра
информационной безопасности
компании «Инфосистемы Джет»



Выбор решения по борьбе с мошенничеством зависит от множества факторов, каждый из которых имеет определенный вес. Выделим наиболее существенные из них.

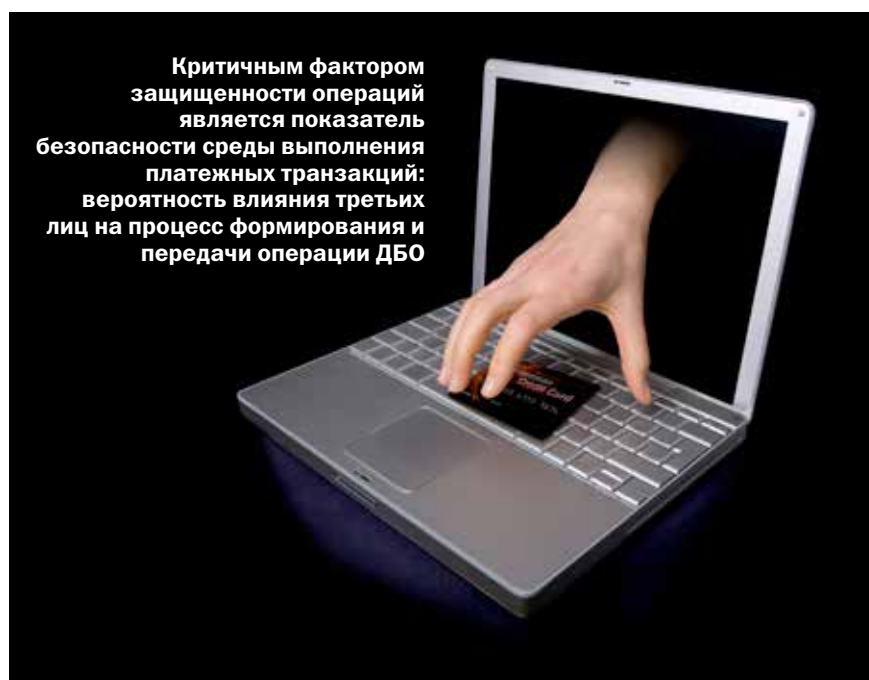
Начнем с деления источников совершения мошенничества на внутренние и внешние. Почему это деление так важно при выборе решения? Потому что оно сказывается на том, какой набор данных нам необходимо собирать для детектирования фактов мошенничества, т.е. где искать следы совершения преступления. К примеру, если речь идет о внешнем мошенничестве, то главным объектом контроля являются транзакции, в том числе и нефинансовые, а «точкой входа» для мошенника, в первую очередь, является стандартный интерфейс бизнес-приложения (контроль удаленных каналов администрирования банковского ПО в этой статье мы не затрагиваем). Для установления факта хищения, совершаемого сотрудником, объектами контроля должны являться внутренние интерфейсы банковского ПО, позволяющие осуществлять несанкционированные изменения или манипуляции с денежными средствами или их источниками. При этом сотрудник может действовать через различные служебные системы и сервисы, что, в свою очередь, отражается на конечном объеме источников данных. Тем самым происходит дифференцирование систем противодействия мошенничеству: на системы защиты клиентских операций и на системы противодействия внутреннему мошенничеству.

Теперь поговорим о каналах, через которые осуществляются незаконные действия (в первую очередь, каналы обслуживания клиентов). К наиболее распро-

страненным относятся каналы ДБО (как юридических, так и физических лиц), процессинговые решения (обслуживание эмиссии банка или эквайринга торгово-сервисных предприятий), обслуживание клиентов в кассовых узлах банка. Сегодня мошеннические схемы перестают ограничиваться отдельным взятым каналом обслуживания. Например, мошенник может воспользоваться технологиями интернет-банкинга для совершения операций между счетами одного клиента, а вывод средств осуществить с помощью карты через банкомат в торговом центре. При этом его действия для процессингового центра будут абсолютно легитимными, если не сопоставлять их с аномальными переводами между счетами в канале интернет-банкинга. Это, в свою очередь, требует от FMS-системы возможности интеграции с различными бизнес-приложениями, а также корреляции событий из разных сервисов в единое приложение

контроля рисков.

Одним из факторов при выборе FMS-решения являются конечные банковские технологии, используемые при обслуживании клиентов в рамках определенного канала обслуживания. Применение той или иной технологии влияет на реализуемые схемы мошенничества. Например, эмиссия банковских карт с микропроцессором повышает устойчивость к компрометации, а осуществление интернет-эквайринга с поддержкой 3D-Secure значительно снижает риски отнесения ответственности по оспариваемым операциям на счет торгово-сервисных предприятий и банка-эквайера. Таким образом, каждый канал характеризуется платежными и операционными рисками, которые напрямую зависят от механизмов обеспечения защищенности совершаемых операций. Наличие любой технологии должно учитываться при настройке системы мониторинга, кроме этого, FMS-система долж-





на обладать потенциальными возможностями настройки под технологии, которые банк только планирует внедрять.

Основной задачей FMS-системы является выявление и предотвращение мошенничества. При этом ее потенциальные возможности по идентификации незаконных операций основаны на функциональности, т.е. на методах формирования политик и правил, способных детектировать хищение. Чем более развиты и гибки инструменты настройки и моделирования в FMS-системе, тем потенциально большие возможности по выявлению мошенничества предоставляются конечному потребителю. Кроме того, FMS-системы должны обеспечивать превен-

тивный характер анализа, что позволяет выявлять не только реализуемые атаки, но и предотвращать готовящиеся хищения за счет исследования процессов на стороне клиента. Таким образом, целью подобных систем будут являться создание механизмов выявления мошенничества еще на этапах его подготовки и минимизация ущерба от атак на начальных стадиях.

Очевидно, что любая FMS-система рассматривает вероятность совершения мошеннических действий на основе данных, полученных для анализа. А поскольку такая система основана на вероятностной модели, так или иначе будут возникать ошибки некорректного выявления мошенничества или его невыявления вовсе. Наступление любого из этих двух событий должно оперативно корректироваться специалистами банка или самой системой. Немаловажными принципами эффективного функционирования FMS-решения являются прозрачность этапов анализа клиентских операций, открытость настройки политик и правил выявления мошеннических действий. Эти характеристики позволяют осуществлять оперативную настройку решения в случае выявления ошибок в его функционировании и тем самым поддерживать необходимый уровень защиты банковских операций.

Следующим фактором, оказывающим влияние на выбор решения, является требование к оперативности реагирования на факт выявления подозрительной операции и составу процедур минимизации ущерба. Если банк осуществляет обработку всех клиентских операций в режиме online или переход к такой модели обслуживания внесен в стратегию развития бизнес-процессов, тогда система мониторинга должна обладать возможностями реакции на события в



режиме реального времени и обеспечивать функционал по приостановке подозрительного действия, блокировке платежного инструмента или счета клиента. Если процесс обслуживания заранее подразумевает временной интервал, на протяжении которого операция «выдерживается» на промежуточном счете, требования по производительности к системе FMS могут быть не столь строгими. Следует отметить, что работа системы предотвращения мошенничества в реальном времени практически всегда требует существования подразделения, функционирующего в режиме 24/7, способного оперативно реагировать на результаты fraud-мониторинга и осуществлять связь с клиентом в случае подозрения на совершение мошеннических операций. Уровень подготовки таких специалистов на самом деле зависит от глубины настроенной математической модели выявления незаконных действий. Если сама модель настроена и поддерживается в актуальном состоянии, и результаты анализа прозрачны, то при существовании механизмов снятия блокировок операций и счетов с задачей контроля работы системы могут справиться рядовые сотрудники call-центра.

FMS-система должна позволять реализовывать задачи в интересах как отдельных подразделений, так и организации в целом. Решение можно рассматривать как надстройку над информационной системой банка, способную решать в том числе аналитические задачи расчета показателей платежных и операционных рисков, выявления тенденций в действиях клиентов и пр. Опыт показывает, что именно процедуры мониторинга платежной



Основной задачей FMS-системы является выявление и предотвращение мошенничества

активности первыми идентифицируют изменения в характере платежных операций всего банка. Кроме того, интеграция решения с системами аналитической обработки или едиными CRM-системами позволяет решать задачи контроля качества обслуживания, развития бизнеса или задачи маркетинга.

Список значимых факторов не ограничивается выше-названными критериями, поскольку он должен учитывать всю совокупность задач, стоящих перед кредитно-финансовой организацией. Поэтому при выборе системы специалисты банка должны четко представлять себе, во-первых, общие стратегические цели развития организации, во-вторых, как будет выстроена ИТ-инфраструктура в соответствии с этими целями и, в-третьих, как будет обеспечена в итоге безопасность бизнеса. ■

Подмена реквизитов платежного поручения, или атака Man-In-The-Browser

Как ни совершенствуются механизмы защиты ПК, как ни развиваются средства выявления вредоносного ПО, основной точкой контроля состояния защищенности ПК являлся и будет являться конечный пользователь. Даже самое совершенное антивирусное ПО не способно полностью запретить установку или внедрение вируса, оно может лишь уведомить о потенциальной угрозе. Таким образом, постоянное совершенствование компьютерных вирусов и троянов, идущее в ногу с развитием методов перехвата управления персональными компьютерами, стало причиной появления отдельного направления в атаках на сервисы ДБО. Такие программы, попадая на компьютер, располагаются между интерфейсом пользователя и бизнес-приложением ДБО. Они способны абсолютно незаметно для клиента осуществлять несанкционированные операции, изменяя отдельные реквизиты в формируемом платежном поручении или внедряясь в процессы подписи документа, а также подменять один документ на другой. Клиент не видит произведенных изменений и сам отправляет мошенническую платежку в банк. Идентификация такого рода атак основывается на выявлении отклонений от истории платежных операций клиента, экспресс-анализе недавно совершенных операций по банку в целом, а также на специфических особенностях формирования платежей такими вирусами.

ПИЛОТИРОВАНИЕ FMS-СИСТЕМЫ ДБО – ФАКТЫ И ЦИФРЫ

АЛЕКСЕЙ СИЗОВ,

архитектор FMRA решений Центра
информационной безопасности
компания «Инфосистемы Джет»

Не секрет, что в России объем мошеннических операций, осуществляемых через каналы ДБО, входит в первую тройку среди видов банковского операционного мошенничества начиная с конца 2009 г. По темпам роста он опережает общий рост объемов платежей всей отрасли в несколько раз. Причины этого – активное развитие новых сервисов и ужесточение требований к безопасности совершения платежных операций «соседних» сегментов клиентского обслуживания: карточного и интернет-эквайринга (за последние 10 лет банковские карты перешли на микропроцессорные технологии, а оплата в сети интернет активно переводится на стандарт 3-D Secure). Достичь необходимого уровня снижения этого показателя только с помощью усиления процедур обеспечения конфиденциальности и целостности данных не удастся. Эффекта не дает и внедрение новых технологий обеспечения аутентичности совершаемых операций. Тем временем суммарные ежегодные,

а иногда и ежеквартальные объемы убытков клиентов стали сопоставимы со стоимостью самых дорогих решений в области защиты сервисов ДБО. Банки сегодня уже пришли к пониманию того, что эффективнее внедрять технологии контроля, не зависящие от клиента, то есть – обладать инструментами выявления мошеннических действий вне зависимости от степени соблюдения клиентом общих требований информационной безопасности.

Наиболее объективную оценку работы системы противодействия мошенничеству, конечно, за исключением этапа ее промышленной эксплуатации, может дать только пилотный проект, во время которого потенциальное решение предварительно настраивается и апробируется на реальных операциях сервиса ДБО. Дело в том, что при внедрении систем Fraud Monitoring необходимо учитывать ряд особенностей. Во-первых, подобные системы отличаются глубокой интеграцией в инфраструктуру ДБО. Фактически они становятся системами

класса Business Critical. Во-вторых, бизнес-показатели по противодействию мошенничеству во многом зависят как от функциональности самой системы, так и от качества работы проектной команды. И, в-третьих, системы Fraud Monitoring'a отличаются сравнительно высокой стоимостью.

Основными целями пилотного проекта являются верификация гибкости встраивания самого решения, его функциональности, профессионализма команды внедрения, а также оценка планируемой эффективности решения. Дополнительно в рамках пилота можно прогнозировать объемы сохраненных средств, необходимость изменения внутренних банковских процедур, а иногда – повысить оперативность внедрения новых банковских технологий.

Кроме того, пилотный проект иногда ставит перед потенциальным заказчиком новый вопрос, параллельный выбору FMS-системы, – выбор системного интегратора, который сможет ре-

ализовать внедрение конечного решения в базовые автоматизированные системы кредитно-финансовой организации. Дело в том, что на успешность внедрения в значительной степени влияют опыт интегратора и квалификация его специалистов, которые обеспечивают качественную техническую и консалтинговую поддержку на всем протяжении внедрения и использования системы FMS.

В чем же особенности проведения пилотного проекта в рамках ДБО? Во-первых, каждая кредитно-финансовая организация имеет свою ярко выраженную специфику ведения бизнеса и использования контрольных процедур при обеспечении безопасности сервисов ДБО. Во-вторых, банки часто обладают уникальным набором сервисов ДБО, сопровождающих их систем, а также политик хранения исторических данных и формирования логов систем. Это исключает возможность унификации состава работ и проведения пилотного проекта по шаблонному сценарию: каждый проект требует базовой настройки компонент загрузки операций ДБО, анализа для определения актуальных мошеннических схем и методов их детектирования, изучения существующих в банке механизмов противодействия мошенничеству.

При этом следует понимать, что пилотный проект – это прежде всего демонстрация возможностей системы на примере частной задачи. Целями пилота могут быть базовая настройка импорта данных в FMS-систему, формирование общих механизмов классификации высокорисковых операций и выявление одного из типов мошенничества. Их достижение позволяет заказчику сформировать представление о принципах интеграции решения

в банковские информационные системы, функциональности логического модуля выявления мошеннических операций, а также об интерфейсах управления.

Мировой опыт проведения проектов показывает, что системы противодействия мошенническим операциям позволяют предотвращать не менее 97% всех атак и не превышают по количеству ложных срабатываний 1% от числа всех операций канала ДБО.

Эти результаты подтверждаются и нашим опытом. Так, например, один из уже завершенных нами проектов по сравнению двух FMS-решений (предлагаемого и реально используемого в банке) продемонстрировал, что современные FSM-системы позволяют детектировать более 98% мошеннических операций и при этом классифицировать как подозрительные только 0,5% операций ДБО. Итоги проекта могут быть переведены и на понятный финансовым организациям язык цифр, а именно: решение позволило предотвратить мошеннические операции на сумму более 3 млн рублей лишь для одного филиала банка, при этом общее количество подозрительных транзакций, выявленных системой, не превысило 0,5% от общего объема операций ДБО.

Таким образом, в случае проектов по созданию и внедрению систем Fraud-monitoring, или Fraud-Management System (FMS), мы можем говорить о прикладной значимости результатов даже «пилотов». Это позволяет банкам оценить ожидаемый результат практически и подойти к решению о старте внедрения системы мониторинга взвешенно, четко представляя соотношение между планируемыми затратами на внедрение и получаемым бизнес-эффектом от пресечения мошеннических действий. ■

Подмена реквизитов платежного поручения с хищением OTP

Практика внедрения технологий одноразовых паролей (One-Time Password – OTP) не осталась незамеченной криминальным сообществом. В настоящее время стали появляться многомодульные троянские программы, целью которых является не только заражение компьютера, с которого формируется платежное поручение сервиса ДБО, но и внедрение вирусов, перехватывающих пароли OTP, например, отправляемые на сотовый телефон клиента. Не секрет, что последние примеры атак на кредитно-финансовые организации характеризуются направленностью на конкретное финансовое учреждение и учитывают уникальные технологии обеспечения защиты ДБО именно в этом банке. Идея атаки заключается в том, что происходит заражение основного компьютера, и если вирус понимает, что используется технология OTP, ожидается поступление информации от вируса, расположенного на сотовом телефоне. Как только OTP поступает на телефон, идет передача пароля на компьютер, где расположен основной вирус. В итоге злоумышленниками осуществляется отправка платежного поручения с легальным OTP с компьютера клиента. Вы спросите, как происходит синхронизация двух вирусов? Вирусы могут идентифицировать друг друга по подключению мобильного устройства к ПК (так зачастую и происходит заражение сотового телефона) или по беспроводным сетям общего доступа. Незамедлительная передача значения OTP в эпоху современных технологий сложности не вызывает. А очередной рубеж защиты операций прорван. Идентификация нового вида атак основывается на выявлении отклонений от истории платежных операций клиента и специфике формирования платежей такими вирусами.

ЗАЩИТА СИСТЕМ ДИСТАНЦИОННОГО БАНКОВСКОГО ОБСЛУЖИВАНИЯ НА БАЗЕ РЕШЕНИЯ ORACLE ADAPTIVE ACCESS MANAGER

ВЛАДИМИР ТОКАРЕВСКИЙ,
руководитель экспертной группы Центра информационной безопасности компании «Инфосистемы Джет»

Информатизация практически всех банковских услуг и консолидация управления счетами в одном бизнес-приложении, доступ к которому осуществляется через интернет, определили рост объемов операций, совершаемых через сервисы удаленного обслуживания. При этом критичным фактором защищенности операций ДБО стал показатель безопасности среды выполнения платежных транзакций (вероятность влияния третьих лиц на процесс формирования и передачи операции ДБО). В первую очередь, должен быть обеспечен высокий уровень безопасности всех информационных ресурсов банка, чьи элементы расположены в пределах сети кредитно-финансовой организации. Банку также необ-

ходимо соответствовать мировым и региональным требованиям по защите информации. В то же время соблюдение требований по защищенности среды осуществления доступа пользователя к банковскому счету и совершения платежных операций зачастую не подконтрольна банку. Тем самым определяются тенденции в развитии схем мошеннических атак: совершенствование механизмов перехвата управления сессией пользователя и подмена реквизитов осуществляемых через каналы ДБО операций. Значительное число таких атак побуждает банки и вендоров разрабатывать механизмы, которые предоставляли бы возможность осуществлять контроль над операциями ДБО, выявлять действия злоумышленников и организовывать методы

усиленной идентификации.

Так, компания Oracle разработала продукт Oracle Adaptive Access Manager (OAAM), обеспечивающий повышенный уровень защищенности бизнес-операций, осуществляемых через каналы ДБО. Решение отвечает тенден-

Назначение Oracle Adaptive Access Manager – проведение анализа всех осуществляемых операций в рамках канала ДБО с целью предотвращения мошеннических действий, а также использования схем дополнительной аутентификации клиента.

циям развития рынка информационных банковских услуг и требованиям по обеспечению защиты персональных и аутентификационных данных клиентов. Как показывает практика, применение решения ОААМ обеспечивает предотвращение до 95% мошеннических операций.

ОААМ – это решение для аналитической обработки всех совершаемых клиентом операций в режиме реального времени. Оно обеспечивает:

- агрегацию данных об операциях, осуществляемых через каналы ДБО, из различных источников;
- анализ этих операций для выявления признаков совершения мошеннических действий;
- формализацию результатов анализа для контроля работы системы и обработки данных о подозрительных случаях.

Одним из основных факторов успешного проведения анализа для выявления мошенничества является полнота доступных данных об операциях канала ДБО. Она обеспечивается за счет использования различных технологий получения данных, в том числе Web Services (SOAP) API, File Loader and Database Loader и др.

Применение этих технологий позволяет не только организовать взаимодействие системы Fraud-мониторинга с сервером ДБО в режиме реального времени, но и предоставляет возможность проектирования механизмов получения данных из внешних источников, напрямую не относящихся к функционированию сервисов ДБО. Как следствие, в схемы анализа могут быть включены данные из таких систем, как АБС, систем back-office и т.д.

Важной особенностью решения является возможность интеграции средств сбора данных (device fingerprints) непосред-

ственно с бизнес-приложением, в котором клиент совершает операции со счетом. Такой подход дает возможность анализировать данные о любых действиях пользователя в рамках приложения с момента его авторизации (подключения к каналу ДБО) и до завершения сеанса. Это позволяет получать более 50 независимых

Под профилем клиента понимается совокупность данных, определяющая его поведенческую модель осуществления операций ДБО. Профиль строится на основании доверенных исторических данных, т.е. истории операций, признанных правомерными, и позволяет рассчитать отклонения от обычного поведения клиента для любой совершаемой транзакции. Это, в свою очередь, отражается на вероятности осуществления мошеннических действий.

параметров среды совершения операции (например, данные о вычислительном ресурсе, с которого осуществлялся доступ к сервисам ДБО) и тем самым усиливать контрольные механизмы за точкой доступа к банковским сервисам.

Основным предназначением ОААМ является выявление и предотвращение совершения мошеннических действий на основе проведения анализа клиентских операций в рамках сервиса ДБО средствами математического моделирования.

Анализ транзакций обеспечи-

вается модулем Risk Engine, который осуществляет:

- формирование профиля клиента;
- проведение анализа по правилам определения подозрительных операций, сформированных банком;
- расчет скорингового балла – показателя вероятности осуществления мошенничества.

Выявление незаконных операций обеспечивается за счет выполнения нескольких классов правил. Во-первых, это правила сравнения параметров анализируемой операции или их группы с заранее заданными пороговыми значениями. В качестве пороговых значений могут выступать, например, превышение допустимой суммы транзакции или осуществление 3 последовательных операций из страны, которая на основании экспертных оценок считается неблагонадежной. Во-вторых, существуют правила выявления отклонений анализируемой операции от профиля клиента по определенным параметрам (например, совершение транзакции в ночное время при отсутствии подобных фактов в исторических данных). Итоговые результаты анализа выражаются в виде скоринговой величины, формируемой совокупностью сработавших правил. Итоговые результаты также могут формироваться после дополнительного уровня анализа, представляющего собой логическую матрицу истинности или ложности всех правил выявления мошеннической операции. Такой подход позволяет контролировать не только факты мошенничества, заложенные в отдельно взятом правиле, но и структурно определять все возможные нарушения установленных банком критериев мошенничества. Это дает возможность более гибко настраивать политики мониторинга операций ДБО.

Отметим, что совокупность



Одним из важнейших факторов построения эффективной модели выявления мошенничества является прозрачность используемых алгоритмов и достоверность результатов анализа

данных профиля клиента и правил, осуществляющих обработку операций в соответствии с этим профилем, является формой самообучения системы. Такая модель позволяет осуществлять автоматизированную оценку совершаемых клиентом операций без модификации правил выявления мошеннических действий.

Одним из важнейших факторов построения эффективной модели выявления мошенничества является прозрачность используемых алгоритмов и достоверность результатов анализа. Здесь стоит отметить, что ОААМ является открытой средой разработки, модификации и настройки политик выявления фактов мошенничества. Решение предоставляет подробную детализацию этапов обработки каждой клиентской транзакции, вплоть до времени выполнения каждого правила. Тем самым достигаются высокие показатели эффективности выявления мошеннических действий, а также минимизация сроков реа-

гирования на новые угрозы ДБО.

Еще одним критерием эффективности работы системы Fraud-мониторинга является производительность решения. ОААМ проектировалось с учетом тенденций увеличения количества и скорости обработки операций ДБО, которые в настоящее время диктуют необходимость проведения большинства операций в режиме online. Решение стабильно функционирует при осуществлении анализа более 100 операций в секунду за счет применения Rete-алгоритма. Кроме этого, в системе предусмотрены механизмы ограничения времени анализа каждой операции, что позволяет предоставить результат во внешние системы по истечении максимально отведенного на анализ срока.

Oracle Adaptive Access Manager обладает широкими функциональными возможностями по выявлению подозрительных операций и автоматизированному реагированию на результаты ана-

Один из компонентов Oracle Adaptive Access Manager – это решение для организации усиленной аутентификации клиента в ключевых точках бизнес-приложения или по результатам анализа его действий. Модуль может работать совместно с любой существующей системой аутентификации, включая:

- статические имена пользователей и пароли;
- генераторы одноразовых паролей от различных поставщиков;
- смарт-карты;
- аутентификация через SMS.

Кроме этого, решение включает в себя серверный компонент и набор виртуальных устройств для web-аутентификации – уникальных форм запроса информации, внешний вид и характеристики которых знает лишь клиент, выбравший их в момент регистрации в системе.

лиза. Решение характеризуется высокими показателями скорости обработки операций и наличием широкого класса средств интеграции со сторонними системами. Таким образом, ОААМ позволяет создавать эффективные системы предотвращения мошеннических действий в рамках канала ДБО с возможностью их масштабирования на новые каналы и технологии обслуживания клиентов. ■



МОШЕННИКИ НЕ ПРОЙДУТ, ИЛИ ВЫЯВЛЕНИЕ МОШЕННИЧЕСТВА С ПОМОЩЬЮ RSA TRANSACTION MONITORING

ВЛАДИМИР ТОКАРЕВСКИЙ,
руководитель экспертной группы Центра информационной
безопасности компании «Инфосистемы Джет»

Мир интернет-мошенничества непрерывно меняется. Новейшие угрозы, такие как атака «человек посередине» (Man-in-the-Middle, или MITM) и троянские программы класса «человек в браузере» (Man-in-the-Browser), быстро развиваются и становятся все более широко распространёнными. Финансовые учреждения по всему миру обязаны реагировать на эти угрозы, создавая мощные, эшелонированные системы обороны. Помимо точной идентификации пользователей, пытающихся войти в систему, важно обеспечить аутентификацию выполняемых ими действий для повышения уровня безопасности online-операций, уменьшения числа мошеннических транзакций и снижения риска от вновь возникающих угроз.

Система RSA Transaction Monitoring предоставляет финансовым учреждениям комплексный набор средств для обнаружения фактов интернет-мошенничества и эффективной борьбы с ним. Она отслеживает поведение пользователей в сети, обнаруживает подозрительные транзакции, позволяет финансовым учреждениям контролировать сомнительные действия в режиме реального времени и принимать соответствующие меры для уменьшения и устранения убытков от мошенничества. Банки могут:

- идентифицировать, противодействовать и анализировать попытки мошенничества без изменения привычных для клиентов систем и процедур;
- добавить к применяемой системе аутентификации клиентов еще один уровень безопасности в виде новых механизмов;

- создать на базе решения RSA систему, которая повысит эффективность противодействия угрозам мошенничества.

ЗА КУЛИСАМИ: МОНИТОРИНГ, ОБНАРУЖЕНИЕ, ПРОТИВОДЕЙСТВИЕ

Ядром RSATransaction Monitoring является самообучающаяся система Risk Engine, которая постоянно контролирует различные действия пользователей и обнаруживает попытки мошенничества. Она в режиме реального времени оценивает любую online-активность пользователей, отслеживая свыше ста индикаторов для надежного обнаружения мошенничества.

Каждому действию присваивается уникальный балл риска в диапазоне от 0 до 1000 на основании байесовой модели¹, которая применяется для автоматической оценки вероятности риска по каждому индикатору. Окончательный балл состоит из следующей суммы: балла зависящего от недавнего поведения; балла, связанного с данными, накопленными за большой период времени; а также балла риска, назначаемого вручную и используемого для борьбы с вновь возникающими угрозами.

RSA Transaction Monitoring проверяет как заранее заданные, так и зависящие от профиля пользователя индикаторы риска. Они используются для уведомления Risk Engine о специфичных для конкретного действия параметрах, несущих информацию о степени риска. Список predetermined индикаторов регулярно обновляется с учетом громадного объема информации, полученной системой Risk Engine, и результатов изучения схемы мошенничества.

НЕКОТОРЫЕ ПРЕОПРЕДЕЛЕННЫЕ ИНДИКАТОРЫ

- eFRAUDNETWORK ПОМОГАЕТ СОПОСТАВИТЬ IP-АДРЕСА И КОНКРЕТНЫЕ УСТРОЙСТВА (ПОЛЬЗОВАТЕЛЬСКИЕ КОМПЬЮТЕРЫ), КОТОРЫЕ РАНЕЕ БЫЛИ ПОМЕЧЕНЫ КАК ОЧЕНЬ РИСКОВАННЫЕ
- Модель поведения пользователя
- Сумма транзакции
- IP-адреса и их география, ранее отмеченные как высокорискованные
- Недавние изменения профиля
- Физическая скорость перемещения терминала пользователя
- Получатели незаконных платежей
- Недавнее открытие счета
- Индикаторы, зависящие от конкретного профиля, используются для выявления аномалий, относящихся именно к нему. Среди них:
 - Идентификационный номер устройства (device ID) и особенности его работы
 - Поставщик услуг в интернете, страна и тип соединения
 - Аномально высокие скорости перемещения терминала пользователя
 - Отклонения от обычного временного режима работы пользователя
 - Тип канала
 - Сумма транзакции
 - Среднее/общее количество операций
 - Предыдущие алгоритмы поведенческих действий

Risk Engine не ограничивается только профилированием пользователей, система анализирует и другие параметры:

¹ Байесовая модель – это вероятностная модель, представляющая собой множество переменных и их вероятностных зависимостей. Она может быть использована для того, чтобы давать ответы на вероятностные вопросы. Например, с помощью модели можно получить новое знание о состоянии подмножества переменных, наблюдая за другими переменными.

- ресурсы, участвующие в транзакции, например, прокси-серверы, другие устройства;
- комбинацию учетной записи пользователя и используемого им ресурса, например, браузера;
- группы учетных записей пользователя (например, все учетные записи, которым соответствуют одинаковые атрибуты профиля). Их использование – один из многих путей, позволяющих системе Risk Engine определять риск даже в тех случаях, когда по отдельному пользователю собрано мало информации.

Алгоритм автоматического распознавания профиля атак способен консолидировать различные параметры и рассчитывать балл риска, используя принцип байесовской сети. Для оценки риска используется статистическая модель, позволяющая учесть все признаки и вычислить вероятность того, что рассматриваемое действие является мошенническим или отличается высокой степенью риска. Параметры байесовской сети ежедневно пересчитываются, что позволяет поддерживать модель в актуальном состоянии.

МОДЕЛЬ САМООБУЧЕНИЯ

Технологии, используемые преступными сообществами для online-мошенничеств, характеризуются высоким уровнем адаптации. Мошенники обладают почти неограниченной мобильностью и потенциально способны в любой момент атаковать любой интернет-портал, используя прокси-сервер для скрытия своих IP-адресов. Принимая во внимание скорость, с которой мошенники изменяют способы своей деятельности, внедрение системы управления рисками, обладающей возможностями самообучения в реальном времени, становится

очень важным фактором.

Как уже было сказано, RSA Transaction Monitoring выявляет факты потенциального мошенничества и присваивает подозрительным действиям высокие баллы риска. Операции с максимальным баллом регистрируются в системе Case Management, работающей в режиме реального времени. Благодаря этому финансовое учреждение имеет возможность контролировать потенциально опасные операции. Результаты исследования немедленно возвращаются в систему Risk Engine, и модель рисков обновляется.

Risk Engine работает в обоих направлениях для снижения коэффициента ложных срабатыва-

БОРЬБА С ВОЗНИКАЮЩИМИ УГРОЗАМИ

Атаки типа «ЧЕЛОВЕК ПОСЕРЕДИНЕ» и трояны «ЧЕЛОВЕК В БРАУЗЕРЕ» представляют собой относительно новые методы, которые используются мошенниками для доступа к информационным системам финансовых учреждений. RSA Transaction Monitoring подготовлена к борьбе как с указанными, так и с потенциальными угрозами. Используя разные способы и компоненты решения (предопределенные и связанные с профилем пользователя индикаторы риска, методики анализа с распознаванием профиля атак, кластеризация и «раскраска», самообучающаяся система Case Management, база данных RSA eFraudNetwork, «учетные записи – ловушки»), Risk Engine обеспечивает защиту финансовых учреждений и их клиентов от постоянно возникающих угроз на длительное время.

ний до минимума. Аналогично тому, как на учет ставятся операции, связанные с подтвержденными мошенническими действиями, регулируется и порядок работы с подозрительными схемами, которым присвоен высокий балл риска и которые в то же время возникли в результате законного поведения пользователя.

ПРЕДУПРЕЖДЕН ЗНАЧИТ ВООРУЖЕН

Возможности Risk Engine расширяются за счет получения данных из международной межкорпоративной базы данных схем и профилей мошенничества RSA eFraudNetwork. Это межкорпоративная сеть, предназначенная для распространения и совместного использования информации о деятельности мошенников. Среди ее членов – десятки международных финансовых организаций, а также некоторые из ведущих мировых поставщиков услуг в интернете. Сообщество eFraudNetwork распространяет сведения о мошенничествах среди многочисленных организаций в режиме реального времени: если атакам мошенников подвергся один из членов сообщества, все остальные немедленно получают об этом уведомления и защищаются от таких атак.

Эта сеть доступна во всех возможных вариантах развертывания RSA Transaction Monitoring. При внедрении системы в Центре обработки данных финансового учреждения локальная копия базы данных eFraudNetwork обновляется каждые несколько минут, обеспечивая заказчиков актуальными сведениями.

RSA Transaction Monitoring помогает работающим в сети RSA транснациональным компаниям – поставщикам финансовых услуг выявлять профили и

схемы атак, отслеживать поведение мошенников более чем в 65 странах. Различные системы RSA в настоящий момент применяют свыше 50 крупных мировых банков, организаций-эмитентов кредитных и дебетовых карт, брокерских фирм и тысячи более мелких финансовых учреждений.

ПОЛИТИЧЕСКИЙ МОМЕНТ

Несмотря на то, что инструменты присвоения баллов риска рассчитаны на обеспечение оптимальной точности (максимальные баллы присваиваются только самым рискованным операциям), компания RSA учитывает, что каждый банк имеет свою собственную специализированную базу знаний и политик управления рисками.

В систему входит приложение Policy Manager, позволяющее организациям формировать собственную модель управления рисками, которая может быть настроена в режиме реального времени. До ввода в действие каждое правило может быть протестировано с помощью средств моделирования на исторических данных и отрегулировано до получения оптимального результата. Кроме того, после ввода в действие каждое правило может быть настроено на обработку ограниченного объема транзакций. Применяя это приложение, финансовые учреждения полностью контролируют свою политику управления рисками.

Помимо прочего, система RSA Transaction Monitoring содержит современные средства управления и дополнительные утилиты, среди которых проблемно-ориентированное приложение Case Management для изучения подозрительных транзакций. Полученное подтверждение о том,

что данная транзакция является попыткой мошенничества или, напротив, идентифицирована как легитимная, автоматически учитывается Risk Engine. Это обеспечивает точную подстройку системы и улучшает характеристики ее работы в будущем.

ВАРИАНТЫ РЕАГИРОВАНИЯ НА ФАКТЫ МОШЕННИЧЕСТВА

При внедрении системы существуют два режима работы: просмотра и принятия решений в реальном времени. В режиме просмотра система обрабатывает каждое действие в реальном времени и передает сведения о подозрительных действиях в приложение Case Management. После этого отдел финансового учреждения, занимающийся борьбой с мошенничествами, обращается к клиентам с просьбой подтвердить законность подозрительных операций. Этот режим является типовым для первого этапа внедрения, однако может быть и штатным в ситуациях, когда финансовые средства не передаются в реальном времени.

В режиме принятия решений в реальном времени, помимо отметки транзакций для просмотра, система генерирует балл риска и рекомендованные меры. После этого финансовое учреждение может использовать результаты работы системы для принятия решения. Стандартными решениями, принимаемыми в реальном времени, являются:

- выполнение транзакции, но присвоение ей отметки для изучения в приложении Case Management;
- задержка транзакции на заданный период времени для изучения с разрешением на выполнение, если изучение не будет завершено вовремя;

РЕЗУЛЬТАТЫ, ПОЛУЧЕННЫЕ ПРИ ONLINE-МОНИТОРИНГЕ БАНКОВСКИХ ОПЕРАЦИЙ В ОДНОМ ИЗ ВЕДУЩИХ ЕВРОПЕЙСКИХ ФИНАНСОВЫХ УЧРЕЖДЕНИЙ:

- СНИЖЕНИЕ ЧИСЛА МОШЕННИЧЕСТВ НА 96%;
- ПРОЦЕНТ ВЫЯВЛЕННЫХ ПОДОЗРИТЕЛЬНЫХ ТРАНЗАКЦИЙ ПО ОТНОШЕНИЮ К ЧИСЛУ ВСЕХ ОПЕРАЦИЙ – 0,2–0,4%;
- КОЭФФИЦИЕНТ ЛОЖНЫХ СРАБАТЫВАНИЙ – 1:880;
- ЗНАЧИТЕЛЬНОЕ СОКРАЩЕНИЕ УБЫТКОВ ОТ МОШЕННИЧЕСТВ И ПОСЛЕДУЮЩИХ ПОПЫТОК НАРУШЕНИЯ ЗАЩИТЫ.

- задержка транзакции на заданный период времени для изучения с запретом на выполнение, если изучение не будет завершено вовремя;
- запрет выполнения операции, которая либо инициирована ресурсом, о котором известно, что им пользуются мошенники, либо связана с аналогичным счетом получателя.

Этот режим работы обычно используется в ситуациях, когда перевод денежных средств выполняется в режиме реального времени и не обратим. Для его применения от программного обеспечения системы ДБО или АБС требуется поддержка режима синхронной работы, например, Web Services (SOAP) API.

За последние несколько лет ряд крупных российских банков вслед за мировыми лидерами рынка оценили возможности RSA Transaction Monitoring. Наш опыт работы с решением показывает, что уровень мошенничества при его использовании действительно снижается. ■

ПРИВЕДЕНИЕ ДВУХ ПРОЦЕССИНГОВЫХ ЦЕНТРОВ КОМПАНИИ «МУЛЬТИКАРТА» В СООТВЕТСТВИЕ С ТРЕБОВАНИЯМИ МЕЖДУНАРОДНОГО СТАНДАРТА БЕЗОПАСНОСТИ В ИНДУСТРИИ ПЛАТЕЖНЫХ КАРТ PCI DSS

ЗАКАЗЧИК

ООО «МультиКарта»:

- создано в 1994г.;
- является дочерним предприятием ОАО Банк ВТБ и входит в Группу ВТБ;
- сертифицировано в качестве третьестороннего процессора и персонализатора в международных платежных системах Visa Int., MasterCard Worldwide;
- лицензировано международными платежными системами Diners Club Int. и American Express на технологическое обеспечение операций с использованием банковских карт.

В настоящее время «МультиКарта» — одна из крупнейших российских процессинговых компаний, обеспечивающая полный комплекс процессинговых услуг для банков и торгово-сервисных предприятий, включая интернет-магазины.

ЗАДАЧИ

Соответствие требованиям стандарта PCI DSS — обязательное требование международных платежных систем, распространяющееся на все организации, которые хранят, обрабатывают, или

передают данные держателей платежных карт.

Компания «МультиКарта» постоянно наращивает свою клиентскую базу и на сегодняшний день оперирует данными платежных карт 38 банков, среди которых — крупнейшие российские эмитенты. Предлагая рынку полный комплекс высокотехнологичных услуг, компания уделяет особое внимание совершенствованию процессов обеспечения информационной безопасности.

В рамках реализации стратегии укрупнения и расширения бизнеса, а также в связи с ро-



«Широкое распространение пластиковых карт – неотъемлемый атрибут современного мира, – комментирует **Иван Твердохлебов, руководитель направления PCI DSS компании «Инфосистемы Джет».** – Но помимо множества удобств, связанных с их использованием, современные технологии имеют и обратную сторону: год от года увеличивается число случаев с карточным мошенничеством. В целях преодоления этой ситуации международные платежные системы принимают различные меры, в том числе разработали единый стандарт безопасности – Payment Card Industry Data Security Standard (PCI DSS) – направленный на то, чтобы минимизировать риски и обеспечить максимальное развитие карточных услуг».

стом нагрузки на существующие вычислительные комплексы, «МультиКарта» завершила проект по созданию нового отказоустойчивого процессингового центра, отвечающего всем требованиям стандарта безопасности в индустрии платежных карт. Партнером в решении задач по обеспечению соответствия нового и действующего процессинговых

Подпись к рисунку вот таким образом. Не забудьте вставить настоящий текст Подпись к рисунку вот таким образом. Не забудьте вставить настоящий текст

«Развитие новых сервисов и обеспечение безопасности операций для держателей карт — одно из приоритетных направлений нашей деятельности, – комментирует **Михаил Федоров, директор по информационной безопасности компании «МультиКарта».** – Благодаря совместной работе по модернизации сетевой и серверной инфраструктуры «МультиКарты», компания «Инфосистемы Джет» досконально знала ее особенности и понимала специфику нашего бизнеса. Помимо этого, компания зарекомендовала себя на рынке как опытный PCI DSS-консультант, успешно реализовавший ряд проектов по приведению в соответствие стандартам процессинговых компаний и банков. Это стало определяющим фактором при выборе интегратора».

центров требованиям стандарта PCI DSS стала компания «Инфосистемы Джет».

РЕШЕНИЕ

Проект был реализован в несколько этапов. Как и в других аналогичных проектах, первоначально было проведено комплексное обследование архитектуры и взаимодействия всех системных компонентов, входящих в состав процессинговой системы. Были определены границы области действия стандарта и разработан подробный план приведения в соответствие с требованиями стандарта.

План работ составлялся сра-

зу для двух процессинговых систем. Специалисты «Инфосистемы Джет» осуществляли проектирование с учетом того, какие решения возможно реализовать на действующем процессинге, а какие – на новом. В этом отношении незаменимой оказалась как поддержка консультантов «Инфосистемы Джет», так и опыт технических специалистов, и знание тех или иных особенностей технологических платформ. Все компоненты будущей системы информационной безопасности строились во взаимосвязи и действительно полезны в повседневной жизни компании.

Второй этап проекта – вне-





«На этом этапе важно определить область предстоящей сертификации – выявить системы, осуществляющие обработку и хранение данных платежных карт, для которых необходимо обеспечить соответствие всем требованиям PCI DSS, – **комментирует заместитель директора Центра информационной**

безопасности компании «Инфосистемы Джет» Евгений Акимов. – Совместно со специалистами компании «МультиКарта» мы составили подробный план работ по приведению в соответствие, включающий комплекс необходимых организационных мероприятий, внедрение новых технических решений и модернизацию. На всех этапах проекта руководство и сотрудники «МультиКарта» шли на открытый диалог, мы обсуждали проектные вопросы и принимали совместные обоснованные решения».



дрение организационных процедур и технических средств обеспечения безопасности. Выполнение части требований стандарта взяла на себя компания «МультиКарта». В частности, специалисты компании вносили изменения в конфигурации функционирующих систем, дорабатывали внутренние регла-

менты и процедуры.

На завершающем этапе отдельная команда специалистов компании «Инфосистемы Джет» провела сертификационный аудит. Проводилась проверка систем, осуществляющих обработку и хранение данных платежных карт, регламентирующих документов и процедур, configura-

ций используемых средств защиты. По результатам составлено заключение о полном соответствии процессинговых центров «МультиКарта» требованиям PCI DSS.

Результаты проведенного аудита были приняты международными платежными системами. Компания «МультиКарта» получила сертификат соответствия требованиям стандарта PCI DSS 2.0.

РЕЗУЛЬТАТ

В настоящее время оба процессинговых центра «МультиКарты» сертифицированы по стандарту PCI DSS 2.0. Наличие сертификата PCI DSS позволяет минимизировать финансовые и репутационные риски, повысить доверие в глазах клиентов, партнеров. Помимо этих преимуществ, соответствие PCI DSS является «сертификатом доверия» от международных платежных систем и означает, что Visa и Mastercard рекомендуют банкам компанию как надежного партнера. **U**

«Мы всегда стремимся обеспечивать высокий уровень оказываемых услуг и предпринимаем шаги по их совершенствованию и поддержке. Выполнение требований PCI DSS свидетельствует о безопасности карточных данных наших клиентов и высоком уровне обеспечения информационной безопасности в нашей компании в целом. Это непрерывный процесс, соответствие необходимо подтверждать ежегодно, и мы планируем продолжить работы по повышению защищенности наших бизнес-процессов», – **подчеркивает Михаил Федоров.**

Противодействие мошенничеству при использовании систем ДБО

АВТОР: ЕВГЕНИЙ АКИМОВ

Развитые сервисы дистанционного банковского обслуживания стали неотъемлемым критерием при выборе банка для клиента. В условиях наращивания функциональности таких систем наблюдается повышение активности преступных сообществ, желающих получить доходы за счет проведения в ДБО мошеннических операций. О том, как обеспечить защиту от мошенничества, рассказал Евгений Акимов, заместитель директора Центра информационной безопасности компании «Инфосистемы Джет».

Источник: Банковские технологии, февраль 2012 г.

ДБО: как защититься от мошенничества

АВТОР: ОКСАНА ДЯЧЕНКО

Сервисы дистанционного банковского обслуживания существуют достаточно давно, но внимание экспертов к проблеме безопасности каналов ДБО обострилось лишь в последние годы. Заместитель директора Центра информационной безопасности компании «Инфосистемы Джет» Евгений Акимов поделился своим мнением о методах минимизации рисков и предотвращения угроз при ДБО.

Источник: Национальный банковский журнал, февраль 2012 г.

Мошенничество в сетях операторов связи. Интерконнект

АВТОР: ДМИТРИЙ ШОПИН

Чтобы у абонентов была возможность звонить и отправлять SMS за пределами своей сети, операторам необходимо организовать интерконнект — взаимное присоединение сетей для обмена трафиком. Этот обмен сопровождается финансовыми взаиморасчетами, а там, где возникают товарно-денежные отношения, появляется возможность мошенничества. Интерконнект-фрод сложен в выявлении и приносит операторам наибольший ущерб. Подробности в статье Дмитрия Шопина, руководителя направления по борьбе с мошенничеством компании «Инфосистемы Джет».

Источник: Стандарт, ноябрь 2011 г.

Не нужно бояться «человека в браузере»

АВТОР: ОЛЕГ СЛЕПОВ

Из всех преступлений в кредитно-финансовой сфере более половины приходится на мошенничество при дистанционном банковском обслуживании. Защита этого сервиса — одна из наиболее важных задач, стоящих перед финансовыми организациями. Обеспечить безопасность в данном случае поможет только комплексное решение, включающее как традиционные меры, так и новые продукты, позволяющие осуществлять более глубокую и интеллектуальную оценку банковских транзакций. Олег Слепов, руководитель направления по борьбе с мошенничеством компании «Инфосистемы Джет», рассказал, что противопоставить угрозам мошенничества.

Источник: BIS, ноябрь 2011 г.

В любой организации есть, что украсть, поэтому всегда найдутся люди, которые будут пытаться это сделать

АВТОР: ОЛЕГ СЛЕПОВ

ИТ-мошенничество стало существенной угрозой для многих российских компаний, независимо от сферы их деятельности. Проблема актуальна для телекоммуникационного сектора, финансовых организаций, топливных компаний и других отраслей нашей экономики. Своим мнением о сложившейся ситуации на рынке информационной безопасности поделился Олег Слепов.

Источник: Antifraudrussia.ru, ноябрь 2011 г.

Фрод - риски операторов связи

АВТОР: ДМИТРИЙ ШОПИН

Границы влияния телеком-фрода на бизнес операторов связи постоянно и стремительно расширяются, охватывая все новые и новые технологии, услуги, сферы деятельности. Методы борьбы с мошенничеством ad hoc — от случая к случаю — больше не оправдывают себя. Все сильнее ощущается потребность в переходе от реагирования к управлению. О существующих способах идентификации фрод-рисков читайте в статье Дмитрия Шопина, руководителя направления Fraud Management & Revenue Assurance компании «Инфосистемы Джет».

Источник: ИКС, май 2011 г.