ITForum 2020/Эволюция

Доверяй, но проверяй

Смутное время — так называют нынешнюю ситуацию игроки банковской индустрии. Непростые условия рынка заставляют банки пересматривать свои ИТ-бюджеты и инвестировать только в то, что необходимо и наиболее эффективно решает задачи бизнеса. При этом банки являются одними из ключевых клиентов ИТ-компаний.

АЛЕКСАНДР КОРЯКОВ

По данным CNews Analytics, сегмент решений для дистанционного банковского обслуживания физических лиц все еще содержит значительный потенциал роста

— безопасность—

Сегодняшнее время участники рынка и аналитики характеризуют как смутное для банковской индустрии. В 2014 году Центробанк продолжит политику оздоровления отрасли. По прогнозу рейтингового агентства «Эксперт РА», кандидатами на отзыв лицензий в текущем году могут оказаться порядка 50 банков. Именно это количество финансовых компаний соответствует хотя бы одному из критериев на вылет. Среди них: достаточность капитала менее 11%, объемы капитала менее 300 млн руб. к 1 января 2015 года, признаки большого количества сомнительных операций.

Обстановка усугубляется тем, что спрос на кредиты начинает уменьшаться, а клиенты стараются перейти в крупные банки, имеются проблемы с ликвидностью, растут объемы проблемных активов.

Банковский сектор все еще растет, но этот рост начинает замедляться. Так, по прогнозу «Эксперт РА», по итогам нынешнего года активы и кредитный портфель в целом по рынку прибавят не более 11% и 13% соответственно. Для сравнения: в прошлом году эти показатели составляли 15% и 17%. Впервые за последние пять лет снизилась совокупная прибыль банковского сектора с 1011,9 млрд руб. в 2012 году до 993,6 млрд в прошлом году. Наряду с этими тенденциями конкуренция между банками обостряется.

Полное досье

В этих непростых условиях банки стремятся к внедрению и использованию информационно-технических средств, которые позволили бы сократить затраты, при этом поддержать лояльность пользователей и повысить продажи за счет правильно сконфигурированных предложений для клиентов.

Евгений Закрепин, первый заместитель управляющего директора компании «Техносерв», говорит, что стремление к экономии средств, в частности желание снизить стоимость обслуживания каждого клиента, проявилось пару лет назад в том, что банки начали активно внедрять единые CRM-системы. Это снимает необходимость обращения к множеству разных программ во время общения с клиентом: вся информация о нем и его взаимоотношениях с банком доступна оператору в одном приложении, причем независимо от того, через какой канал коммуникаций он обратился (офис обслуживания, телефон, онлайн-чат и т. д.).

Такие возможности достигаются, только если банк позаботился о создании интегрированной информационной системы всего своего предприятия. По словам господина Закрепина, именно внедрение интеграционных шин — это то, чем продолжает заниматься банковская отрасль в 2014 году. Эти технические средства позволяют разрабатывать универсальные интеграционные сервисы и осуществлять обмен информацией между системами. При такой организации корпоративной инфраструктуры становится неважно, какая именно система и от какого вендора используется в банке в данный момент и будет ли она заменена.

Стоимость обслуживания на одного клиента также может быть снижена за счет перевода пользователей в цифровые каналы и каналы самообслуживания. Интернет-банкинг продолжит активно развиваться не только потому, что это более удобный интерфейс для современного человека, но и потому, что это гораздо менее затратный способ взаимодействия банка с потребителем по сравнению с оффлайновыми отделениями, где работают высокооплачиваемые специалисты. Так, по планам ВТБ 24 к 2016 году банк будет обслуживать через онлайн-кабинет 4 млн человек, что в три раза больше, чем по показателям второго полугодия 2013 года. К 2017 году каждая седьмая операция будет осуществляться с помощью интернет-банка. Такие показатели намечены в стратегии развития ВТБ 24 на 2013-2016 годы. В середине прошлого года 7% операций банка приходилось на онлайн-кабинет.

По данным CNews Analytics, сегмент решений для дистанционного банковского обслуживания (ДБО) физических лиц все еще содержит значительный потенциал роста. В 2013 году всего 85% банков, входящих в топ-100 использовали такие системы. Наибольшую популярность получила система типа интернет-банк, которая внедрена у 83% банков топ-100 против 79,8% в 2012 году. Заметно выросла популярность решений для мобильного банкинга: их в 2013 году использовали в 64% банков топ-100 против 54,1% годом ранее.

Опасные связи

Помимо тренда на сокращение стоимости обслуживания, который чудесным образом ведет и к повышению лояльности потребителей (если онлайн- и мобильный банкинг удобны), также финансовые организации все больше вынуждены тратить на обеспечение безопасности. Потери от мошенничества, фрода, инсайдеров и воровства растут в том числе потому, что развивается рынок онлайновых платежей.

По данным исследования B2B International, проведенного совместно с «Лабораторией Касперского» в 2013 году, 98% пользователей используют онлайн-финансовые сервисы, при этом почти треть из них не проверяет те сайты, на которых вводит свою конфиденциальную информацию. Безусловно, возможность получить доступ и контроль над финансовой информацией и счетами пользователя привлекает злоумышленников.

«В 2013 году нашими продуктами было заблокировано 1,9 млн атак банковским вредоносным ПО. Все это приносит серьезный ущерб и пользователю, и репутации банка, на клиента которого была произведена атака», — рассказывает Владимир Заполянский, руководитель отдела технологического позиционирования «Лаборатории Касперского».

Согласно тому же исследованию, за предшествующий год с киберугрозами, нацеленными на получение доступа к онлайн-счетам, в мире столкнулись 62% пользователей, а в России — 74%. В 2013 году произошли значительные изменения, связанные с усовершенствованием законодательства, активными действиями правоохранительных органов разных стран, которые вывели из строя некоторые наиболее одиозные преступные группы. Тем не менее, как рассказывает господин Заполянский, место крупных игроков криминального рынка стали занимать мелкие группировки и все большее количество мошенников стало обращать внимание на финансовые организации. В целом мировая тенденция такова, что системы ДБО банков атакуются все чаще.

При этом банковские угрозы быстро эволюционируют не только с точки зрения их количества, главное — они становятся все более сложными. Безусловно, банки осуществляют ряд эффективных мер по борьбе с онлайн-мошенничествами, такие, как CVV2, двухфакторная аутентификация, токены и другие, но, по мнению господина Заполянского, для эффективного противостояния современным угрозам этого не достаточно. Злоумышленники научились обходить двухфакторную аутентификацию просто и эффективно. Крупные банки используют защиту на стороне серверной инфраструктуры, но при этом не учитывается тот факт, что наиболее уязвимое звено при совершении онлайн-операции — это пользователь, поэтому его устройство необходимо защищать в первую очередь.

«Финансовым организациям необходим комплексный подход, который бы защищал онлайн-операцию и на конечном устройстве пользователя, и на стороне банка (на случай, если у пользователя не установлено защитного решения). Кроме того, очень важно, чтобы банковские эксперты обладали последней информацией об актуальных способах атак и знали, как именно нужно построить эффективную защиту», — говорит господин Заполянский.

Помимо направлений, связанных с обслуживанием потребителей и обеспечением защиты, банковский сектор, как и раньше, будет продолжать выделять бюджеты на соответствие требованиям регуляторов. В целом игроки ИТ-рынка рассчитывают на то, что бюджеты кредитных организаций на ИТ в 2014 году не уменьшатся.

Светлана Рагимова

Новые киберугрозы для бизнеса

— экспертное мнение —

Ежегодно специалистами проводятся исследования в области киберугроз и их опасности для бизнеса. Год от года эти киберугрозы только растут. При этом многие считают, что целевые атаки являются проблемой лишь крупных компаний, особенно тех, которые обеспечивают работу особо важных для страны объектов инфраструктуры. Но ведь абсолютно все предприятия имеют дело с информацией, способной заинтересовать киберпреступников, поэтому в действительности мишенью злоумышленников может оказаться любая организация.

Ни для кого не секрет, что защита информации зиждется на трех китах — конфиденциальности, целостности и доступности. Причем работа любой организации в настоящее время сопряжена как с работой на корпоративных ресурсах, где хранится часто конфиденциальная информация (КИ), так и с использованием BYOD-устройств*, где также хранится КИ. Электронная почта, облачные сервисы, сайт-компании — основные атрибуты современного бизнеса любого уровня. Все это — объекты для злоумышленников. Сами угрозы из года в год трансформируются, приобретая новые формы исполнения. Это и так называемые «зловреды» (вредоносное ПО), и DDOS-атаки, отказ в обслуживании, незакрытые уязвимости в приложениях (JAVA-уязвимости, Adobe Reader).

Так, по последним данным, в мире 91% компаний сталкивались с киберугрозами за последние 12 месяцев. Причем 48% считают киберугрозы одним из трех наиболее значимых рисков для бизнеса. При этом все равно можно утверждать, что на сегодняшний день абсолютное большинство компаний недооценивают масштабы современных киберугроз. Так, например, в 2013 году «Лаборатория Касперского» провела опрос среди крупных компаний о частоте появления новых вредоносных программ. Близкую к реальным показателям оценку дали лишь 4% опрошенных, в то время как около 95% занизили цифру. А между тем ежедневно в мире появляется около 200 тыс. вредоносных программ.

Руководствуясь только этими данными, сложно дать объективную оценку готовности компаний к защите от инцидентов информационной безопасности. Тем не менее адекватная оценка уровня угроз может оказать серьезное влияние на решения, которые компания принимает при выборе средств для защиты своей IT-инфраструктуры. Действительно, антивирусная защита — наиболее распространенная мера для обеспечения информационной безопасности IT-инфраструктуры в компаниях любых размеров по всему миру. Но это далеко не всё.

Сегодня, например, большинство современных компаний хранят свои данные в «облаке», что позволяет значительно экономить средства. Плюс такого хранения также в том, что это дает гибкость для работы с данными (доступ в любое время из любой точки мира и с любого устройства), но и мишенью злоумышленников облачные сервисы становятся всё чаще. Необходимо понимать, что организации могут использовать сторонние ресурсы для обработки и хранения информации, но все равно продолжают нести полную ответственность за свои данные.

«Облака» подвержены широкому спектру атак: подмена метаданных, wrapping attack, вредоносные инъекции в код, вредоносные инъекции в базы данных, межсайтовый скриптинг, DDoS-атаки и DNS-атаки. Особенно облачные сервисы чувствительны к DDoS-атакам. Атаки на отказ в облуживании — это возможность сделать компьютерные ресурсы недоступными для пользователей, для которых они предназначены. Достаточно сложно отличить легитимный трафик от нежелательного. Определение и фильтрация атак — это достаточно весомая задача в такой среде, как облачные вычисления, где все виртуализировано. Нет ни одной технологии, которая полностью может отфильтровать DDoS-атаку. Если системы провайдера услуг будут взломаны и произойдет утечка информации, то ответственность за утрату данных будет лежать на компании. Следовательно, предприятия должны оценивать потенциальные риски хранения данных на стороне точно так же, как если бы они хранили данные в пределах собственной IT-инфраструктуры. Одно из самых немаловажных значений имеет фактическое местонахождение серверов, на которых хранятся данные организации, и соответствующая юрисдикция, под которую они при этом подпадают.

Также на безопасность бизнеса серьезно влияет растущая популярность смартфонов. IT-службам теперь приходится обеспечивать безопасность разнообразных устройств в составе корпоративной сети: ПК, ноутбуков и смартфонов различных моделей. Проблема усугубляется тем, что многие сотрудники используют одно и то же устройство как в личных, так и в рабочих целях — тенденция BYOD (Bring Your Own Device). В связи с этим утеря мобильного устройства и хранящихся на нем данных грозит серьезными последствиями не только для самого владельца смартфона, но и для организации, в которой он работает. Речь идет об утечке конфиденциальных данных, а также возможном ущербе для репутации компании. Таким образом, потенциальные риски связаны не только с угрозами, исходящими от вредоносных программ, но и с возможной утечкой данных в результате утери или кражи мобильного устройства сотрудника. Несомненным преимуществом компании МТС было внедрение сервисов безопасности для абонентов, а именно — антиDDoS, «Родительский контроль», «Чистый интернет», управляемые межсетевые экраны, managed VPN, антивирус, антиСПАМ, антиФРОД и т.п. Принятие превентивных мер на собственных или корпоративных смартфонах сегодня играет немаловажную роль. Необходимо формирование зоны безопасности вокруг каждого сотрудника, независимо от того, откуда и с какого устройства он работает. А защитные инструменты, используемые в организации, должны быть достаточно гибкими для успешного применения такой политики «индивидуальной защиты».

Не сделаю открытие, если скажу, что современные угрозы в высшей степени сложны. Однако часто целевая атака начинается с обмана и втирания в доверие к конкретному сотруднику той или иной компании, что сразу ставит под угрозу всю компанию. Киберпреступники часто собирают необходимую им информацию в соцсетях, а затем используют ее, чтобы проникнуть в корпоративную сеть, зная о наличии конкретных барьерных методах защиты. Социальная инженерия процветает активно, сотрудники просто не осознают существующую опасность, а это значит, что человеческий фактор активно процветает и при постановке вопроса о киберугрозах. Данный фактор обязательно нужно учитывать при формировании стратегии ИБ. А начинать нужно с повышения осведомленности сотрудников в вопросах информационной безопасности.

Екатерина Старостина, главный эксперт отдела защиты конфиденциальной информации департамента информационной безопасности компании МТС