ТРЕНДЫ ФИНАНСОВОЙ ИНДУСТРИИ: ЗАЩИТА ДАННЫХ, BIGDATA, МОБИЛЬНЫЕ ПЛАТЕЖИ

Алексей НАЙДА,
директор по развитию бизнеса
ООО «Эффективные
информационные технологии»

Исторически финансовая индустрия всегда старается использовать передовой опыт в борьбе со злоумышленниками. Банки уже умеют надежно защищать как пользовательские данные, так и свои коммерческие. Порядка 98% данных, которые могут быть скомпрометированными, находится исключительно в базах данных.

Конфиденциальная информация, как правило, собирается и хранится приложением в производственной среде. Однако проблемы защиты данных выходят далеко за рамки производственных систем. На каждую единицу конфиденциальной информации в производственной среде приходится множество копий, которые распространяются как «вверх» – для разработки ПО и тестирования, так и «вниз» – для анализа и построения отчетов. В конечном итоге такие копии составляют 80 % и более всей конфиденциальной информации. В связи с этим актуальность использования систем деперсонализации (маскирования) данных возрастает с каждым годом. Маскирование данных позволяет полностью сохранить актуальность типов и форматов данных, что удобно для разработчиков и аналитиков. Но при этом данные не отображают реальной информации, и тем самым становятся полностью бесполезными для злоумышленников.

Лидеры финансовой индустрии всегда стараются использовать передовой опыт в борьбе со злоумышленниками. Банки уже умеют надежно защищать как пользовательские данные, так и свои, коммерческие. Порядка 98% данных, которые могут быть скомпрометированы, размещены исключительно в базах данных. В связи с этим актуальность использования систем деперсонализации (маскировки) данных возрастает с каждым годом. Маскировка данных позволяет полностью сохранить актуальность типов и форматов данных, что удобно для разработчиков и аналитиков. Но при этом данные не отображают реальной информации, и тем самым становятся полностью бесполезными для злоумышленников.

За последние 20 лет данная область знаний в сфере обеспечения безопасности информационных технологий существенно эволюционировала. Стоимость цифровых носителей информации стала копеечной, скорость доступа к информации – моментальной, что упрощает создание собственных дата-центров в крупных финансовых компаниях.

Ежегодно банки и финансовые компании вкладывают огромные деньги в обеспечение безопасности как внутри, так и снаружи периметра. В данной отрасли уже давно существует огромный класс стандартов и экспертных знаний. Международные платежные системы (Visa, MasterCard) вкладывают миллиарды долларов только на поддержание всех своих инфраструктур строго в рамках данных стандартов, в разработку и развитие которых они вкладывают деньги такого же масштаба. Современные криптостойкие алгоритмы шифрования и размеры ключей позволяют практически гарантировать стойкость шифрованных данных к подбору ключа, так как на это злоумышленнику понадобилось бы пару сотен лет. Инфраструктуры информационных систем настолько усложнились, что для проведения серьезных атак злоумышленники вынуждены объединяться в группы и действовать на своих «зонах ответственности». Именно поэтому среди них все более популярны различные методы применения социальной инженерии (использования человеческого фактора). Именно поэтому многие финансовые структуры внедряют двухфакторные аутентификации, интеллектуальные системы мониторинга и отслеживания различных аномалий в системе, таких как:

Денис КИРИЧЕНКО,
СТО, Компания «InterKassa»

нетипичное поведения клиента, движение денежных средств, анализ трафика и т. п.

Банки все больше вкладывают денег в обучение персонала и повышение осведомленности своих клиентов в сфере конфиденциальности личных и корпоративных данных, снижении риска утечки информации из-за безграмотности в вопросах безопасности.

Юрий КУЧЕР,
Руководитель службы поддержки
клиентов компании «Интеллика»

Снижать операционные издержки и повышать эффективность обслуживания нужно прежде всего развитием каналов ДБО и обучению клиентов пользоваться ими. Инвестировать во фронты отделений нужно не с точки зрения оптимизации процессов, а с точки зрения доставки знаний о клиенте сотруднику отделения – какой продукт нужно и можно продать клиенту с учетом его истории и потребности в настоящий момент, что необходимо сделать с точки зрения послепродажного обслуживания. Интересно и результативно с точки зрения лояльности клиента проактивное обслуживание, когда банк решает потенциальную проблему еще до момента ее наступления. Например, клиент пришел оформлять депозит, при этом у него заканчивается срок действия карточки через несколько месяцев, а динамика посещений отделений и пользования продуктами подсказывает, что за перевыпуском ему придется специально посещать банк. Инструменты предиктивной аналитики должны подсказать операционисту, что лучше порекомендовать сделать перевыпуск уже сейчас, а еще лучше, если карта уже заранее перевыпущена и нужно только отдать ее клиенту. Вот в такие технологии «умного» фронт-офиса эффективней инвестировать, а не экономить копейки на пресловутом «едином окне».

Экономить затраты за счет CRM и фронт-офиса было актуально 5-10 лет назад. Сейчас эффективней улучшать Customer Experience за счет инструментов RealTime аналитики, предиктивного анализа, чтобы обеспечить тот самый «нужный продукт в нужное время в нужном месте». Технологии BigData и DataMining наконец позволили это делать. В Украине ни один банк, кроме Приватбанка, даже близко не подошел к использованию инструментов и подходов BigData в своей деятельности. В то же время, для хранения и передачи информации существует целый ряд требований и рекомендаций как международных платежных систем, так и НБУ. Достаточно их выполнять, как минимум.

Появление на рынке новых платежных инструментов заставляет производителей POS-терминалов быстрее реагировать на изменения рынка и активнее предлагать новые сервисы. Однако, и рынок не так прост. Согласно новому исследованию компании International Data Corporation (IDC), в 2017 году мобильные платежи во всем мире достигнут объема $1 трлн, а это в два раза больше, чем прогнозируемые $500 млрд в 2015 году.

Следует сказать, что эксперты и аналитики в своей оценке могут и ошибаться. Например, к 2008 году прогнозировалось, что объем таких платежей составит 37 млрд долларов, в то время как в 2009 их объем был зафиксирован на уровне 10 млрд долларов.

В чем аналитики не ошибаются, так это в том, что рост будет достигнут за счет платежей через мобильные устройства. Ведь пользователям удобнее совершать платежи со смартфона в удобное для них время, используя специальные приложения и не выходя на улицу. Так, недавно в Украине было представлено бесплатное приложение MobiPay для смартфонов. Для начала использования мобильного кошелька MobiPay достаточно добавить в него свою платежную карту Visa или MasterCard, при этом все данные карт хранятся на сертифицированных PCI DSS серверах.

Дмитрий КАЛЕНЫХ,
Заместитель генерального
директора компании АМИ

Александр ПЕТРИЧЕНКО
Кандидат технических наук,
Генеральный директор
компании ProfITsoft

Наша компания занимается разработкой системы, позволяющей осуществлять бесконтактные платежи посредством мобильного телефона и технологии NFC. Это удобно, так как не обязательно носить с собой пластиковые карты – все они доступны в нужный момент в мобильном телефоне. Это безопасно, так как для осуществления транзакций используются одноразовые ключи с ограниченным сроком действия, все данные передаются и хранятся в зашифрованном виде, а для подтверждения транзакции клиент должен ввести мобильный PIN-код.

Схема работы следующая. Клиент, являющийся клиентом одного или нескольких банков-партнеров, устанавливает себе специальное мобильное приложение на телефон, проходит процедуру регистрации, подключает свои платежные карты или заказывает новую мгновенную карту. Для этих карт формируются и загружаются на телефон данные, позволяющие осуществлять транзакции. После этого, клиент может расплачиваться за покупки, просто поднеся телефон к платежному терминалу и введя PIN-код.