На «сером» рынке баз данных набирают популярность информационно медицинские продукты – картотеки полисов ОМС, истории болезни, мобильные телефоны пациентов частных и государственных клиник. Предложения доступны на «пиратских» рынках, в интернет магазинах и уже пользуются спросом у широкого круга покупателей – от фармкомпаний до туроператоров и агентств ритуальных услуг. VM сделал контрольные закупки некоторых товарных единиц информационной линейки и попытался разобраться, где начинаются их поставки. ОМС МАРКЕТИНГНа Савеловском рынке базы данных предлагают две точки с соответствующей вывеской, управляемые ИП «Ароян». Хит продаж – многофункциональные базы, включающие сразу реестры паспортных данных, водительских удостоверений и полисов ОМС. Такие продукты здесь реализуются отдельно по субъектам РФ. Например, диск с базой данных по Московской области обошелся VM в 1,5 тысячи рублей. Реестр ОМС на нем включает основную персональную информацию всех жителей этого региона: адрес и дату рождения страхователя, номер его полиса и СНИЛС. «Если вам нужны данные только ОМС, попробуем собрать базу по всем регионам. Выйдет не дороже 10 тысяч рублей», – пояснил скидочную политику продавец одной из точек и, чтобы развеять сомнения, тут же показал выгрузку такой базы в формате excel на своем ноутбуке.
Помимо картотеки ОМС, в ассортиментной линейке есть еще один продукт – «Медстрах». Кроме базовых персональных данных, этот реестр дополнен информацией об организации или ведомстве, которое покрывает человеку расходы по страховке. Стоимость такого предложения тоже находится в диапазоне 1,5 2 тысячи рублей.
Сотрудники территориальных ФОМС и страховых компаний, опрошенные VM, утверждают, что им о продажах баз на свободном рынке ничего не известно. «Вероятно, произошла утечка информации, но точно не от нас», – дистанцируется от темы сотрудник отдела безопасности ФОМС Владимирской области. Представители федерального ФОМС на запрос VM не ответили. Продавцы на Савеловском, естественно, не раскрывают ни своих поставщиков, ни клиентов, ограничиваясь прикладными рекомендациями: «Мы же не спрашиваем вас, зачем вам базы данных. Но если вы, например, из фармкомпании, то возьмите лучше базы абонентов сотовых операторов – сможете рекламу по SMS рассылать».
Савеловский рынок считается сейчас крупнейшей точкой продаж «серых» информационных баз. С ним конкурируют только «Горбушка» в Москве, городские рынки в регионах и интернет магазины, в которых, правда, представлены совсем другие продукты. Например, сайт bazabd.ru предлагает базы психбольных Башкирии, наркоманов и психбольных Барнаула, пациентов медучреждений Тольятти и другие аналогичные картотеки, стоимость которых варьируется от 300 до 1 тысячи рублей. Помимо паспортных данных, в предлагаемых реестрах можно найти номера мобильных телефонов и адреса проживания указанных пациентов.
В профильных IT компаниях говорят, что данные в эти каналы продаж поступают в результате разного рода утечек из соответствующих учреждений, а количество «сливов» только в сегменте медуслуг уже достигает нескольких десятков в год. Например, по оценкам InfoWatch, в прошлом году медицина входила в число отраслей лидеров по количеству информационных утечек с долей 8,3% от всех информационных потерь. По этому показателю она уступала только направлениям торговли, гостинично ресторанных услуг, банковскому сектору и госорганам. «Исследования основаны, как правило, на открытых источниках и показывают лишь

верхушку айсберга. Реальный масштаб утечек может быть в разы больше», – отмечает руководитель аналитического центра компании Zecurion Владимир Ульянов.

ПРОТИВ ВЕТРА

Информационные потери начали фиксироваться в сегменте медуслуг еще с 90-х годов. «Первые утечки происходили случайно, но в основном были связаны с утерей бумажных документов, и в них не было подоплеки мошенничества. Такие случаи происходят и до сих пор», – говорит Владимир Ульянов из Zecurion. С ним соглашается ведущий эксперт компании InfoWatch по информационной безопасности Андрей Прозоров: «Чаще всего бумажные медицинские карты просто выбрасывают. Это классический пример российского раздолбайства и наплевательства».

Некоторые случаи утечек по небрежности получили широкий резонанс и даже привлекли внимание правоохранительных органов. Прошлой зимой в Ханты-Мансийском автономном округе ксерокопии паспортов, СНИЛС и страховых медицинских полисов пациентов Сургутской городской поликлиники №4 оказались разбросаны по городскому парку «Кедровый лог». Как выяснилось, документы перевозились в архив медучреждения, и при погрузке часть бумаг просто унесло ветром. Инцидент получил всероссийскую огласку, и руководство ЛПУ было вынуждено принять строгие административные меры. «Ответственное лицо, из-за которого в лечебном учреждении произошла такая оказия, было уволено», – сообщили VM в поликлинике.

Позже в городе Лангепасе того же Ханты-Мансийского автономного округа врач стоматологической клиники «Дентал» забыл амбулаторную карту пациентки в такси. Дальнейшего распространения персональных данных не произошло, водитель такси, обнаруживший карту, сразу позвонил по указанному в ней телефону. Тем не менее пациентка обратилась в региональную прокуратуру с требованием привлечь к ответственности медучреждение. В результате в отношении клиники и врача были возбуждены административные дела по ст. 13.11 КоАП РФ. Правда, по итогам рассмотрения дел, как сообщили VM в региональной прокуратуре, все ограничилось лишь вынесением предупреждения врачу и медучреждению.

Представители компаний, специализирующихся на информационной безопасности, отмечают, что случайные утраты бумажных документов в сегменте здравоохранения, как правило, не имеют серьезных последствий ни для виновных, ни для потерпевших. Гораздо масштабнее ущерб от учащающихся преднамеренных электронных утечек из медицинских информационных систем.

Волна краж оцифрованных персональных данных начала подниматься в середине 2000-х параллельно с активным внедрением медицинских информационных систем. По данным компании Inline Technologies, уже в первой половине 2008 года потери бумажных данных занимали только 10% от общего объема утечек в медицинских информационных системах, остальное приходилось на CD, DVD, флеш-накопители, серверы настольных компьютеров, ноутбуки, КПК и другие электронные носители информации. При этом злонамеренные «сливы» составляли уже почти треть всех случаев потери данных в сегменте медицинских услуг.

Самой распространенной причиной электронных утечек IT-эксперты называют кражу. «Красть могут врачи, потому как имеют прямой доступ к информации плюс материальную заинтересованность. Не секрет, что многие врачи взаимодействуют с фармкомпаниями и – обычно на какой-то платной основе – рекламируют тот или иной препарат. И если фармкомпаниям будут необходимы какие-то списки по пациентам,

некоторые медики могут согласиться на кражу баз данных пациентов, особенно если им будет предложена значительная сумма», – рассказывает Андрей Прозоров из InfoWatch. О хакерских атаках на информационные системы в сегменте медуслуг, по его словам, пока говорить не приходится. Схожего мнения придерживается директор по развитию КМИС Александр Гусев: «Редко когда это бывают какие-то технические вещи или взломы систем безопасности».

В числе заказчиков «слива» персональной информации из медучреждений, говорит Андрей Прозоров, помимо фармкомпаний, фигурируют и обыкновенные мошенники, которые, получая доступ к базам данных пациентов, звонят им, предлагая купить «эффективное» лекарственное средство от их заболевания. Кроме того, персональные данные пациентов, в частности, их диагнозы, могут быть интересны компаниям, предлагающим, например, туры на оздоровительные курорты. «Получая доступ к базе данных пациентов больниц, они обзванивают их, пытаясь мотивировать к поездке на один из таких курортов, иногда предлагая скидки для людей с конкретным диагнозом. Есть свой интереси у ритуальных агентств – они готовы платить за обновление базы умерших пациентов, чтобы оперативно предлагать родственникам свои услуги», – рассказывает Прозоров. Но наибольший интерес для кражи, по словам эксперта, представляют персональные данные знаменитостей: «Эту информацию готовы покупать, а значит, может найтись человек, который готов ее продавать». Ценники в России, конечно, поскромнее, чем 50 тысяч евро, предложенные за историю болезни Михаэля Шумахера, но спрос на медкарты отечественных селебрити растет.

Нарастание волны утечек эксперты объясняют как минимум двумя причинами – несовершенством медицинских информационных систем и слабостью законодательной базы. Сейчас безопасность личной медицинской информации в России подпадает под действие ФЗ №152 от 27 июля 2006 года «О персональных данных». Ответственность за безопасное хранение и распространение информации о своих пациентах – как в электронном, так и в любом другом виде – возложена этим законом на медучреждения. Отдельные технические требования к защите персональных данных в информационных системах прописаны в постановлениях ФСТЭК №21 и №17.

Правда, санкции за потерю персональных данных пока невелики: максимальное наказание, которое можно получить по ст. 13.11 КоАП РФ «Нарушение установленного законом порядка сбора, хранения, использования или распространения информации о гражданах (персональных данных)», ограничивается штрафом до 1 тысячи рублей для должностных лиц и до 10 тысяч рублей – для юридических. По мнению экспертов из IT-компаний, подобная либеральность косвенно поддерживает низкий уровень защиты персональной информации в сегменте медуслуг.

ЗАЩИТНЫЕ РЕАКЦИИ

Найти учреждения медсектора, откуда происходят утечки персональных данных, непросто. Опрошенные VM участники рынка медуслуг не комментируют состояние своей информационной безопасности или утверждают, что не сталкиваются с проблемой утраты данных. Однако представители IT-компаний зафиксировали в последние несколько лет всплеск заказов на услуги защиты данных именно со стороны медучреждений. «Если три года назад клиентов из этой отрасли у нас вообще не было, то теперь мы начали работать с клиниками, которым устанавливаем DLP-системы и другие заслоны от внешних вмешательств. И часто утечки информации фиксируются уже на этапе внедрения наших систем», – рассказывает Владимир Ульянов из Zecurion.

Представитель компании «Информзащита» Андрей Тимошенко говорит, что частные клиники начали обращаться в его компанию три года назад: «До этого они пытались решать вопросы по защите персональных данных, в частности, данных о состоянии здоровья, самостоятельно. А в 2011 году у нас пошел вал клиентов, в том числе работающих в медицинском сегменте».

Компания «ДиалогНаука» два года назад заключила контракт с крупной столичной клиникой «Медицина» на приведение ее информационной системы в соответствие с международным стандартом защиты информации ISO/IEC 27001. «Соответствие такому стандарту позво ляет оптимизировать расходы на безопасность, риски, связанные с возможными ущербами для активов предприятия, операционные затраты», – считает гендиректор компании «ДиалогНаука» Виктор Сердюк.

Усилили внимание к вопросам защиты данных и территориальные отделения ФОМС. «Мы начали осуществлять отдельные проекты по информационной безопасности еще в 2007 году, а два года спустя внедрили комплексную систему защиты, вся информация фонда про ходит по зашифрованным каналам, и утечки исключены», – говорит представитель ТФОМС Владимирской области. Его коллега из ТФОМС Оренбургской области говорит о подобных мероприятиях, проведенных примерно в тот же период: «Мы создали отдел информацион ной безопасности, прописали организационно распределительные документы, внедрили технологии защиты персональных данных DLP». Представители фондов предполагают, что источником утечки данных о страхователях могут быть их партнерские страховые компа нии. Страховщики, опрошенные VM, такое предположение опровергают. «Случаев утечки у нас не было. В компании существует многоуровневая система защиты информации, которая предотвращает доступ к данным пользователей, не имеющих на это прав», – заверяет директор по маркетингу направления «Медицина» компании «АльфаСтрахование» Егор Сафрыгин. А топ менеджер другой страховой компании говорит, что источником утечек медицинской информации, вероятнее всего, могут быть государственные медицинские информационные системы.

Представители государственных поставщиков ЕГИСЗ утверждают, что утечки исключены. «Существующая защита информации подразумевает комплекс мер, включающий регламенты, аппаратные средства защиты безопасности, софт», – убежден представитель компании «Ростелеком».

На периферии ситуация с информационной безопасностью неоднородна. Как сообщил VM источник, близкий к воронежскому МИАЦ, в регионе действует многоуровневая система защиты данных: «Никогда не встречал баз данных пациентов – ни на «Горбушке» в Воронеже, нигде, хотя одно время мы специ ально мониторили пиратские диски с базами данных, но пациентских баз мы не находили». На некоторых территориях страны о защите персональных медицинских данных говорить и вовсе не приходится, поскольку сама система ЕГИСЗ пока находится там на начальном этапе инсталляции. Например, ответственные за работу ЕГИСЗ подразделения администрации Ленобласти в мае только разрабатывали план по ее внедрению. Интересно, знают ли региональные чиновники, что на сайте bazabd. ru базу персональных данных 10 тысяч пациентов Ленинградской области можно без проблем приобрести за 1 тысячу рублей.

www.pandora.medsteg.ru