Российское подразделение известной швейцарской страховой компании «Цюрих» может оказаться в центре скандала. По данным «Известий», злоумышленники похитили полные данные более чем на 1 млн ее клиентов, заключивших за последние 1,5 года договоры страхования. Источники в правоохранительных органах сообщили, что мошенники пытаются найти покупателей на эту базу и есть вероятность, что она окажется в распоряжении нелегальных фирм, специализирующихся на торговле базами данных. Эксперты считают, что столь крупная клиентская база может быть также интересна как конкурирующим страховым компаниям, так и криминальному миру.

– В руках преступников оказались более чем 1 млн личных дел, в которых, среди прочего, указаны полные данные, адреса, места работы и мобильные телефоны людей, которые заключили с «Цюрихом» различные договоры о страховании, – рассказал источник в правоохранительных органах.

Примечательно, что украденная база данных совсем свежая: в нее вошли клиенты, которые воспользовались услугами компании с января 2012 года по февраль 2013-го, то есть многие страховые договоры сейчас актуальны.

Точная дата утечки информации из СК «Цюрих» неизвестна. Также пока нет информации о том, кто, как и откуда скачал данные клиентов. По словам оперативников, они проводят проверку – кому сведения, украденные у страховщиков, могли быть проданы.

В российском представительстве страховой компании «Цюрих» информацию о похищении базы данных клиентов комментируют осторожно и избегают прямых ответов.

– СК «Цюрих» уделяет первостепенное внимание безопасности персональных данных наших клиентов, – заявил «Известиям» гендиректор компании Николай Клековкин. – Мы расследуем любые случаи, когда безопасность подобных данных находится под угрозой, и в случае необходимости информируем об этом правоохранительные органы.

В МВД «Известиям» сообщили, что пока не располагают данными о похищении

клиентской базы «Цюриха».

В компании Натальи Касперской InfoWatch, занимающейся информационной безопасностью организаций, оценили утечку как крупную.

– Миллион клиентов – это очень приличная утечка. При правильном использовании базы можно легко за год переманить 60–70% клиентов в другую компанию, – сообщил «Известиям» исполнительный директор компании InfoWatch Всеволод Иванов. – В зависимости от портфеля потери могут исчисляться десятками и сотнями миллионов долларов.

Всеволод Иванов отметил, что страховые данные могут представлять интерес как для бизнесменов, так и для криминального мира.

– Во-первых, клиентскую базу можно перепродать конкурентам, – пояснил «Известиям» Всеволод Иванов. – Во-вторых, там есть данные об автомобилях, которые могут быть востребованы у угонщиков. В-третьих, это данные по неурегулированным убыткам и отказанным возмещениям для продажи адвокатам с целью обжалования в суде. Наконец, это информация по обязательному и добровольному медстрахованию с историями болезни для перепродажи фармкомпаниям для таргетированного маркетинга препаратов. Сейчас это очень актуальная проблема.

Примечательно, что международная компания «Цюрих» в 2008 году уже оказывалась в центре скандала. Тогда британское отделение страховой компании Zurich Insurance призналось в утечке данных более полумиллиона своих клиентов. Данные были утеряны во время транспортировки в центр хранения на территории Южной Африки. За это управление по финансовым услугам Великобритании обязало страховую компанию выплатить рекордный штраф в размере £2,3 млн.

Если данные клиентов были действительно похищены из российского филиала «Цюриха», то вряд ли это грозит страховщикам суровым наказанием. По словам специалистов InfoWatch, в России также предусмотрены штрафы, но не за сам инцидент с персональными данными, а за нарушение порядка их защиты.

– Утечки же как таковые наказания не влекут, о чем свидетельствуют компьютерные диски с персональными данными, которые в изобилии лежат на прилавках рынков, – говорят в компании.

В беседе с «Известиями» член комитета Госдумы по информационной политике, информационным технологиям и связи Роберт Шлегель отметил, что одно лишь ужесточение ответственности для компаний за утрату данных не поможет переломить ситуацию.

– Что касается штрафов, то надо понимать, что и сами потерпевшие, чьи данные были утеряны, могут подавать в суд и требовать от компании те суммы, которые считают необходимыми, – пояснил Шлегель. – Однако кроме усиления ответственности за утечки необходимо еще и усилить безопасность компаний. Например, переходить на отечественный софт и оборудование. Пока мы пользуемся западным, мы не может быть уверены, что посторонние люди не получат доступ к нашей информации.

В компании Group-IB, помогающей российским киберполицейским в борьбе с виртуальной преступностью, описали три основных сценария, по которым происходит утечка данных из компаний.

– Первый вариант – это утеря или похищение ноутбука, на котором хранились данные, – рассказал «Известиям» заместитель руководителя лаборатории компьютерной криминалистки компании Group-IB Сергей Никитин. – Однако в России в отличие от Запада не развит рынок целенаправленной охоты за информацией, поэтому подобный сценарий маловероятен. Более правдоподобен второй вариант: базу данных клиентов мог прихватить с собой уволенный сотрудник. Наконец, третий вариант – это заражение компьютеров компании вредоносными программами, вследствие чего хакеры получили доступ к базе данных, поняли, что у них в руках золотая жила, и похитили информацию.

Сергей Никитин отмечает, что для каждого из этих сценариев существует эффективный способ защитить свои данные.

– Если речь идет о краже или похищении ноутбука, то поможет шифрование данных, – рассказывает Сергей Никитин. – От недобросовестных сотрудников поможет внедрение систем защиты, которые позволяют отслеживать, куда уходит информация: кто ее копирует или пытается выгрузить из базы данных. Даже если злоумышленник все же успеет украсть информацию, его всегда можно будет найти.

Наконец, по словам Никитина, наиболее распространенный вариант – заражение вирусами.

– В этом случае надо понимать, что многие сотрудники в рабочее время заходят на развлекательные сайты, где для заражения достаточно просто пройти по случайной ссылке, – говорит Никитин. – После этого заражается не только компьютер, но и вся сеть. Проблема в том, что в некоторых компаниях системные администраторы забывают обновлять установленный на компьютерах софт, а сами пользователи сделать этого не могут, поскольку у них нет прав администратора. Необновленное ПО делает компьютер уязвимым для вирусов.

Примечательно, что исследования экспертов InfoWatch показывают, что в 2012 году число зарегистрированных утечек конфиденциальной информации из российских компаний и госорганизаций выросло в пять раз – до 74 случаев. При этом, по словам экспертов, это верхушка айсберга: всего лишь 1–2% от реального числа утечек становятся известны.

Проблему усугубляет специфическое видение российскими работниками своей роли в компании.

– Оказалось, что среди опрошенных сотрудников отделов продаж и менеджеров по работе с клиентами 92% считают базу данных клиентов компании своей личной собственностью, – говорит Всеволод Иванов. – Это означает, что если такой сотрудник по какой-либо причине покинет компанию, он заберет с собой эту базу, что может нанести серьезный удар по бизнесу. Вообще же 76% опрошенных полагают, что использование чужих клиентских баз данных – это нормальный инструмент ведения бизнеса.

Симптоматично то, говорят в InfoWatch, что эта цифра практически совпадает с данными о проценте злонамеренных утечек от их общего числа в российских компаниях – 77%.

Источник: Известия , 26.07.13