ИНСТРУМЕНТЫ, ЦИФРОВЫЕ ТЕХНОЛОГИИ, СВЯЗЬ, ИЗМЕРЕНИЯ

Что делать, если утечка информации уже случилась?

27 июня 2014 г. в 12:38

Даже одна и даже незначительная утечка информации может повлечь за собой серьезные неприятности для успешно функционирующего предприятия. Ущерб от такой утечки может быть разным, например: в виде крупных финансовых потерь или удара по имиджу и репутации компании. Именно поэтому большинство современных предприятий с особым вниманием подходят к вопросам обеспечения безопасности своих данных. Но, несмотря на усилия, вложенные в обеспечение информационной безопасности, уберечься от утечек удается не всегда. Что делать, если утечка все же произошла?

Негативные последствия или вред от утечки данных

Для того чтобы побороть последствия утечки данных, нужно сперва определить на сколько важными эти данные были для компании и какую ценность имели. Данный анализ даст понять уровень ущерба, который может принести произошедшая утечка. Далее все действия сводятся к минимизации ущерба, примеры которого мы сейчас рассмотрим.

Самый очевидный ущерб, который может принести утечка информации — это финансовые убытки. Если ваши конфиденциальные данные попадут в руки конкурентов, то им это может пойти на пользу, а вам естественно — нет. Чтобы четче представить данную ситуацию приведем наглядный пример. Компания «Росток» разработала новую технологию изготовления лейки. Теперь лейка компании вмещает объем воды гораздо больший, чем ее аналоги у конкурентов, при этом она лучше адаптирована для пользователя. Даже с повышенным объемом воды держать ее действительно удобнее, чем аналоги конкурентов. А насадки на горлышко лейки адаптированы под разные растения и способны не только комфортно их поливать, но и вода через них струится особенно. Одним словом, сказка. Руководители компании в предвкушении, что совсем скоро «взорвут» рынок садовых инструментов и радостно потирают руки. Но вот незадача. Уже завтра конкуренты выпускают такие же лейки с такой же самой технологией, как и компании «Росток». Потребитель ринулся скупать лейки, а компания «Росток» выпала в осадок. А оно ведь и понятно. Все средства, усилия и время, вложенные в разработку лейки, были потрачены впустую. Другими словами, компания «Росток» славно потрудилась на благо

конкурентов. Таким образом, компания-разработчик пострадала не только в финансовом плане, но и в плане развития. Еще более худшим развитием сценария может стать обвинение конкурентом реального разработчика технологии в плагиате. Тогда компания «Росток» потеряет уже не только вложенные средства и доверие пользователей, но и возможность производства леек по своей технологии. В лучшем случае, в данной ситуации, продажи лейки компании «Росток» будут значительно меньше ожидаемых.

Другим негативным последствием, образовавшимся в результате утечки данных, могут стать судебные иски пострадавших. В данном случае речь идет об утечке персональных данных. Как показывает практика, судебные иски также приносят серьезные финансовые убытки компаниям. Однако этим дело может не ограничиться. Вслед за финансовыми убытками от судебных исков могут последовать штрафы от регулирующих органов, занимающихся защитой персональных данных.

На постсоветском пространстве проблема штрафов еще не так актуальна, как в западных странах, но постепенно мы приближаемся к ответственности за информационные потери.

Еще одним серьезным убытком для предприятия из-за утечки информации станет удар по репутации. Любая организация, допустившая хищение информации, ухудшает свой имидж в глазах потенциальных клиентов, партнеров и собственных сотрудников. Все это в перспективе может привести к недополученной прибыли и оттоку квалифицированных кадров, что даже хуже недополученных денег. Репутационные потери особенно актуальны для компаний, работающих на западных рынках, либо в сфере, связанной с защитой данных. Часто именно репутационные потери оказываются самыми болезненными. Еще хуже будет, если утечка информации произошла в переломный для организации период, тогда потеря данных информации может стать причиной банкротства.

Последовательность действий при утечке информации

Для борьбы с последствиями от утечки данных стоит предпринять следующие меры:

1. определить источник утечки информации, чтобы в будущем аналогичный инцидент не повторился;
2. выяснить круг лиц, которым стала доступна похищенная информация;
3. установить, какие еще данные могли быть скомпрометированы в результате этой утечки;
4. оповестить о хищении информации лиц, которые могут от нее пострадать;
5. при необходимости обратиться в правоохранительные органы;
6. вести работу над минимизацией ущерба по каждому из возможных направлений.

Вкратце рассмотрим каждый из пунктов поподробнее.

Определить виновника утечки информации можно посредством анализа сетевой активности пользователей корпоративной компьютерной сети. Выполнить это можно с помощью системы мониторинга информационных потоков предприятия или DLP-системы (от англ. Data Leak Prevention — защита от утечек данных).

Далее следует выяснить, кто получил конфиденциальные сведения, чтобы понять, кому и чем это грозит. Дать конкретные советы здесь будет трудно, так как все зависит и от самой информации и от ее получателя. Стоит понимать, что одно дело, когда утечка данных произошла об исследовании рынка и совсем другое — когда список крупнейших клиентов попадает в руки ближайшего конкурента.

После этого стоит оценить, какие еще данные могли передать за пределы компании те, кто виновен в первой утечке. Это, опять-таки, нужно для того, чтобы более полно оценить последствия последней для самой фирмы и других, связанных с ней организаций и частных лиц.

Четвертый пункт становится для многих компаний самым сложным, так как никто не любит признавать собственные ошибки. Большинство организаций предпочитают утаивать информацию об утечки данных, чтобы минимизировать ее последствия, но на самом деле достигают противоположного эффекта. Не сообщая об утечках тем, кто может пострадать от них, компания не дает возможности своим клиентам, партнерам и сотрудникам защититься. Как следствие, доверие и лояльность к такой компании теряется, если общественность узнает о случившемся инциденте.

В зависимости от серьезности утечки информации не лишним будет обратиться в правоохранительные органы, чтобы наказать виновных. Однако стоит помнить, что практика судебного преследования виновных в разглашении коммерческой тайны не слишком распространена, поэтому компании предпочитают решать вопросы касательно утечек информации самостоятельно. Как следствие, отсутствуют показательные судебные процессы, способные заставить задуматься сотрудников, прежде чем совершать хищение информации.

Минимизация ущерба

После того, как риски просчитаны, действия спланированы, стоит приступить непосредственно к действиям по снижению ущерба, вызванного утечкой информации. Для начала будет рационально ускорить выполнение бизнес-процессов, в которых вращаются похищенные данные. Ведь, когда бизнес-процессы завершены, то данная информация теряет свою актуальность, как следствие, и не может нанести серьезный ущерб компании. Так, возвращаясь к примеру с компанией «Росток», можно ускорить вывод на рынок разработанную модель лейки, чтобы опередить конкурента. Если производство и поставки

товара в магазины потребуют гораздо больше времени, сил и средств, то начать заранее рекламную компанию, продемонстрировать образец на профильных выставках, а также как можно громче заявить о своей разработке, — под силу практически каждому. Подобные шаги помогут минимизировать, недополученную в результате хищения информации, прибыль. Аналогичные действия актуальны не только для технологических разработок, но также и для маркетинговых исследований, бизнес-планов и других документов.

Последствия утечки информации можно также уменьшить, если достаточно громко об этом заявить. Причем назвать не только ее виновников, но и заказчиков. Делать это нужно только в том случае, если у вас есть неопровержимые доказательства причастности конкурирующих организаций к утечке, в противном случае вас могут обвинить в клевете и оштрафовать на солидную сумму. Если доказательства причастности конкурентов к утечке данных у вас есть, то ваша компания при заявлении об этом будет выглядеть даже в более выигрышном свете, чем та, по инициативе которой, это произошло.

Для защиты от судебных исков, а также для минимизации расходов на компенсацию ущерба от утечки данных стоит своевременно предупредить о ней пострадавших клиентов, партнеров и сотрудников. Также неплохо «работает» предложение денежной компенсации. Данные затраты буду значительно меньше суммы возможных исков. Однако, чтобы желающих получить компенсацию не было слишком много, можно организовать ее выдачу по паспортам. Как известно, люди не очень любят «халяву», когда для ее получения требуется документ.

Повлиять на испорченную репутацию можно, если продемонстрировать свою человечность. Во-первых, предоставить публике наказанного виновника. Во-вторых, рассказать о действиях, которые компания совершает для предотвращения подобного инцидента в будущем. В-третьих, провести, например, благотворительную акцию по сбору пожертвований в детский дом.

Итоги

Утечка информации может случиться в любой компании. Главное здесь не впадать в отчаяние, своевременно принять меры по ее устранению, а также сделать соответствующие выводы. Если в компании произошла утечка данных, то стоит понимать, что это недоработка сразу во многих областях, начиная с кадровой политики и заканчивая непосредственно контролем работы сотрудников на их рабочих местах.

В целом, если подойти к решению проблемы с умом, то можно снизить последствия даже очень крупной потери данных, а если повезет — улучшить свое положение и наказать конкурента.