Как в Украине защитить свой бизнес от мошенников и инсайдеров?

PUBLISHED 22 ВЕРЕСНЯ 2013

Утечки информации есть везде, где есть бизнес. Украина – не исключение. Поэтому решать только вам, какой ценностью обладают конфиденциальные данные в вашей компании, и стоит ли тратить усилия и средства на обеспечение безопасности данной информации.

Разъяснение политик безопасности

Компания SearchInform провела исследовательский проект на тему информационной безопасности в Украине, России и Латвии. Более 1200 респондентов было опрошено в рамках проекта. О том, в каком состоянии пребывает информационная безопасность в украинских компаниях, мы и поговорим дальше.

Инсайдерская активность для Украины явление не новое. Так, например, выборы в верховную раду Украины в 2012 году запомнились повышенным интересом мошенников к персональным данным обычных граждан. На 86 УИК в Киеве во время подачи документов кандидатур в состав участковых комиссий от партии «Правая воля Украины» было определено, что документы составлены на основе персональных данных управления образования Голосеевского района. Однако мошенничества по политическим мотивам не ограничились сугубо Киевом. В Тернопольской области в каждом из округов были также зафиксированы массовые фальсификации и подделки избирательной документации, а также мошенничества при проведении жеребьёвки в ОИК и УИК.

Утечка конфиденциальных данных при проведении политических мероприятий

носит временный характер и зависит собственно от периода, когда они проводятся, а вот утечка данных в бизнес среде явление постоянное. Явление, которое вынуждает руководителей предприятий быть бдительными и принимать меры по обеспечению сохранности своих данных, так как в обратном случае даже одна утечка информации может нанести серьёзный удар по имиджу и репутации компании.

Согласно результатам исследования компании SearchInform, в 86% украинских организаций проводится инструктаж сотрудников для разъяснения политик информационной безопасности. Этот же показатель в России составляет 69%. В Латвии данный показатель аналогичен украинской действительности. Там инструктаж среди своих сотрудников проводят на 1% меньше компаний.

Однако разъяснение политик информационной безопасности среди сотрудников не может дать гарантию, что после данного мероприятия все станут «шёлковыми» и «ласковыми», а при обнаружении инсайдера в тот же миг побегут в службу информационной безопасности компании. Как известно, правила существуют, чтобы их нарушать.

Поэтому можно поверить в добродетель и искренность своих сотрудников, а можно вдобавок к этому перестраховаться. Как говорится, доверяй, но проверяй. Именно поэтому многие компании для

обеспечения безопасности своих данных используют DLP-системы (от англ. DataLeakPrevention). Данные системы предназначены для контроля и фильтрации всего исходящего и входящего трафика по каналам связи, которые используются в компании.

Некоторые работодатели заранее предупреждают своих сотрудников о наличии на предприятии данных систем, некоторые работодатели предпочитают эту информацию скрывать. Естественно, если человека предупредить, что за ним следят, он будет этого остерегаться и стараться не совершать глупостей, тем самым угроза утечки данных с его стороны будет минимизирована. Если же человека не предупреждать о наличии DLP, то в скором времени можно будет понять, как он относится к правилам информационной безопасности предприятия.

Ликвидация угроз

Тайная слежка за активностью сотрудника посредством DLP-системы может вызвать ряд спорных вопросов на тему: а не нарушает ли работодатель закон о вторжении в частную жизнь человека? Прежде всего, данные системы нацелены на выявление случаев, связанных с инсайдом, т.е. они устанавливают факт утечки информации как таковой, а не лезут в личную жизнь человека. Кроме того, работодатель имеет право знать, чем занимается его подчинённый в рабочее время.

Также при трудоустройстве работник подписывает соответствующие документы, где его предупреждают об обеспечении информационной безопасности на предприятии, поэтому подписывая такие документы, он соглашается с корпоративными правилами. Сами же разработчики DLP-систем рекомендуют работодателям умалчивать о наличии в компании DLP-системы, так как в таком случае она даст больше плодов. Однако стоит понимать, что работник будет сильнее мотивирован не совершать глупостей, зная, что за ним следят.

Согласно исследованию SearchInform, 77% украинских компаний предупреждают своих сотрудников о наличии на предприятии DLP-систем. В России и Латвии работодатели предпочитают действовать ровно противоположным способом. Там о наличии DLP-систем знают сотрудники 38% опрошенных компаний в России и 40% – в Латвии.

Однако комплекс мер, направленный на предотвращение утечек данных, всё равно не даёт гарантии, что попытки хищения информации не будут предприняты со стороны сотрудников. Согласно исследовательскому проекту SearchInform, в Киеве за минувший год наиболее склонными к краже корпоративной информации оказались менеджеры (38%), IT-специалисты (15%) и специалисты финансового сектора (13%). Для сравнения этот показатель не сильно отличается от показателя в России.

Данные исследования отличаются только в финансовом секторе. Так по вине финансистов в России в 3 раза больше происходит утечек данных, чем в Украине. В Латвии же на первом месте – менеджеры (32%), далее следуют IT-специалисты и финансисты (по 21%). Наибольший же соблазн украинские мошенники испытывают к краже финансовой (36 %), персональной (28 %) и технической информации (17 %). Эта классическая тройка остается неизменной вот уже несколько лет, распределяя лишь между собой «призовые места». Аналогичная ситуация зафиксирована в России и Латвии.

Уровень информативности

С тем, кто больше всего склонен к краже корпоративных данных, а также какие именно данные чаще всего подвергаются хищению, мы разобрались. Теперь стоит разобраться, какие каналы передачи данных

больше всего контролируются в компаниях, а значит, какие каналы представляют наибольший риск утечки информации.

В 2012 году наиболее контролируемыми каналами связи в опрошенных украинских компаниях стали: электронная почта (38%), веб-браузеры (19%), носители CD/DVD/USB (18%), интернет-мессенджеры (ICQ, Jabber, QIPи т.д.) (12%), Skype (4%).К примеру, особую популярность сегодня получают чаты социальных сетей, которые благодаря интеграции с портативными мобильными устройствами обрели широкое признание и массовую любовь пользователей. Интернет-мессенджеры также занимают особое положение в коммуникационном процессе, так как просты в применении и совместимы со всевозможными системными платформами.

Если инцидент кражи информации всё же имел место быть, многие компании, как правило, предупреждают об этом своих клиентов. Некоторые организации предупреждают о возможных угрозах своих клиентов, а также приносят извинения. Некоторые компании обращаются в СМИ, чтобы предостеречь своих клиентов. Многие компании предпочитают умалчивать и скрывать факты утечки данных. В Украине как раз доминирует третий случай.

Согласно проведённому исследованию, 74% опрошенных компаний заявили, что в случае утечки информации они не сообщали об этом своим клиентам, так как были уверены, что утечка не принесёт вреда. 22% опрошенных компаний сообщали об утечках своим клиентам и приносили извинения. В СМИ об утечках данных заявили бы 4% опрошенных компаний, однако прежде с такой практикой не сталкивались.

Таким образом, утечки информации есть везде, где есть бизнес. Украина не стала тому исключением. Статистика же говорит о том, что проблема утечки конфиденциальных данных остаётся по-прежнему актуальной не только для компании из Украины, но и для компаний из других стран. Поэтому решать только вам, какой ценностью обладают конфиденциальные данные в вашей компании, и стоит ли тратить усилия и средства на обеспечение безопасности данной информации.

Автор: Кикеня Максим, компания SearchInform, **Финобзор**