«Эксперт Северо-Запад» №37 (434) / 28 сентября 2009

Решение для всех

Алексей Леонтьев, корреспондент журнала «Эксперт Северо-Запад»

Подход к вопросу обеспечения информационной безопасности должен сочетать различные оценки подразделений компании

Тезис, что в постиндустриальной экономике информация становится ключевой ценностью компании, оспариванию не подлежит. Для многих она и продукт, и средство производства. Информационные ресурсы, которыми владеет бизнес, позволяют ему получать значительные доходы. С другой стороны, потери, возникающие в компаниях вследствие хищения этих ресурсов, также колоссальны. В условиях кризиса, как показывает и мировая, и отечественная статистика, риски, связанные с потерей информации, растут. Число компаний, желающих любым способом убрать с рынка конкурентов, равно как и сотрудников, планирующих если не обрушить бизнес, то по крайней мере отомстить предприятию, которое несправедливо с ними поступило, заметно растет. Собирая круглый стол, посвященный проблеме информационной безопасности (модератором выступил генеральный директор компании iPipL Дмитрий Петров), «Эксперт Северо-Запад» намеренно отказался от обсуждения узких проблем этого сегмента ИТ.

Закон и рынок

В начале дискуссии в центре внимания экспертов оказались не требования и реалии рынка, а требования государства. Сегодня проблема информационной безопасности становится максимально актуальной благодаря вступлению в силу ряда законов, ее прямо затрагивающих, заметил петербургский представитель группы компаний «Информзащита» Вадим Кропотов. Для таких видов информации, как персональные данные и коммерческая тайна, государством не только установлены требования, как именно их защищать, но и назначен час икс – 1 января 2010 года. «И надо заметить, что федеральный Закон о персональных данных касается буквально всех. У всех есть отделы кадров, у всех есть клиенты. Даже частнопрактикующий зубной врач, если он ведет базу данных клиентов на ПК, попадает под действие закона, то есть должен обеспечить надлежащий уровень защиты», – рассказывает Кропотов.

Во многом аналогичная ситуация складывается и с информацией, представляющей коммерческую тайну. «С 1 января 2010 года начинает работать также Закон об открытости органов государственной власти и местного самоуправления, – продолжает Вадим Кропотов. – По закону если информация не защищена режимом коммерческой тайны, то и госорганы не должны ее защищать, более того, обязаны предоставить ее любому интересующемуся. То есть информация легко может перейти к конкурентам». Проблема в том, что режим коммерческой тайны – не просто соответствующий гриф на пакете с документами, а комплекс нормативных актов, регулирующих режим коммерческой тайны в компании.

Безусловно, эти законы несопоставимы по степени влияния на бизнес. Необходимость введения режима коммерческой тайны уже осознана многими компаниями и без подсказки государства. В конечном счете для большинства это единовременное мероприятие, которое к тому же позволит лучше организовать работу компании. Закон

о персональных данных предполагает и на порядок больший объем изначальных вложений, и их регулярность.

Впрочем, хотя данный закон, без сомнения, серьезное явление для всех компаний, не стоит его излишне демонизировать. Он содержит и необходимые оговорки, которые оставляют бизнесменам пространство для маневра. «Не нужно чрезмерно сгущать ситуацию с Законом о персональных данных, – считает технический директор компании „ВЭЛЛ-КОМ“ Владимир Подзоров. – Федеральная служба по техническому и экспертному контролю выпустила конкретные требования к уровню защиты в зависимости от типов персональных данных, но в ее предписаниях есть ряд важных оговорок. В частности, когда речь идет о клиентской базе, если данные обезличены, не содержат исчерпывающей информации о клиенте, то государство не требует строго соблюдать определенный им порядок обеспечения безопасности». Таким образом, проблема защиты информации, представляющей коммерческую тайну, для бизнеса все же более актуальна.

Познай самого себя

«На уровне бытовой логики, наверное, все понимают, какие виды информации следует защищать. Это финансовая информация, базы данных клиентов и поставщиков, информация, касающаяся ноу-хау и специфики видов деятельности (банков, страховщиков и т.д.)», – полагает директор отдела информационных технологий компании «Смарт Телеком» Константин Перминов. Но переход от общего понимания к конкретным действиям по защите информации зачастую непрост. «Прежде чем приступить к защите от каких-либо угроз, бизнес должен определить, какая информация для него ключевая. Собственно модель защиты строится от определения защищаемых данных», – объясняет технический специалист отдела системной интеграции компании «Поликом Про» Кирилл Случанко.

Правильно оценить стоимость информационных ресурсов может только та организация, которая ими владеет, уверен директор центра защиты информации компании «Конфидент» Егор Кожемяка. «Любая внешняя компания, которая придет в качестве консультанта, будет проводить аудит и все равно начнет с вопросов к заказчику: „Сколько стоит этот ресурс?“, „Есть ли статистика инцидентов?“, „Какие у вас были потери?“ и т.д.», – поясняет Кожемяка.

На первый взгляд это кажется простым – выделить данные, утеря которых может фатальным образом сказаться на деятельности компании. Но на деле, замечает начальник отдела информационной безопасности компании «Севкабель-Холдинг» Егор Чемоданов, для любой организации, маленькой или большой, составление конкретного перечня документов, которые надо защищать, – очень сложный процесс. «Как это происходит, например, в большой компании: собирают руководителей всех подразделений и ставят перед ними задачу определить данные, которые необходимо сохранить. В первом списке оказывается много лишнего, он переписывается еще несколько раз, и только с четвертой или пятой попытки определяется лишь та информация, которую действительно необходимо защитить. И изначальный перечень из 17 листов помещается на половине листа», – рассказывает Чемоданов.

Второй логичный шаг — определение того, как оценить потенциальные риски и, соответственно, какие средства можно потратить на защиту. Тут, как считает Егор Кожемяка, есть два возможных пути. Можно защищаться по требованиями нормативных документов и законодательства, в частности ГОСТов. Сейчас особенно актуален закон

о защите персональных данных, раньше востребованными были работы по приведению системы информационной безопасности в соответствие со стандартами, в частности международными. С другой стороны, можно провести анализ рисков, учесть либо качественную, либо количественную оценку потенциального ущерба. И в зависимости от этих оценок строить систему управления рисками, понимая, сколько денег можно потратить на то или иное решение. «Если отталкиваться от экономического подхода к оценке защиты, то прежде всего необходим тщательный анализ рисков. Если смотреть на вопрос в черно-белых тонах – защищать или нет, – то можно опереться на требования стандартов», – подытоживает Кожемяка.

Но вряд ли кто-то сегодня будет просто принимать принципиальное решение защититься от угрозы. Защищать свою информацию будет бизнесмен, четко понимающий, что потерять он может несоизмеримо больше, чем потратит на информзащиту. «В основном аспекте подход со стороны и малого, и крупного бизнеса одинаков. Все идет от денег. Для чего мы выстраиваем производственные процессы, создаем ноу-хау? Чтобы зарабатывать деньги. Для чего мы нанимаем сотрудников? Для того же. Для крупных компаний, особенно государственных, технологический процесс – это все, поэтому он и защищен по полной», – рассуждает коммерческий директор компании «ЛАНК Телеком» Алексей Максимихин.

Скрытая угроза

Расчеты расчетами, но есть элемент защиты, который очень сложно определить с помощью привлеченных специалистов, – поступки сотрудников. «Если риски остановки процессов или утери данных могут быть снижены в чисто технологической области, то вопрос с уходом данных более сложен и не замыкается на компьютерных технологиях. Он выходит на уровень взаимодействия человека с компьютером и человека с человеком. А такие риски более сложно предотвратить, и, скорее всего, именно они будут иметь более весомые последствия», – делится Константин Перминов. Поэтому предотвращение утечки данных находится в самом «темном углу» процесса обеспечения безопасности.

По данным компании Gartner, 70% всех потерь – это инсайд, то есть потери от действий работников предприятия. «Больше половины из этого – не умышленный вред, а халатность. У нас ситуация не сильно отличается от общемировой», – уточняет Вадим Кропотов. «Опыт показывает, что большое количество сотрудников, отвечающих за сохранность информационных систем (более половины), согласно различным опросам, готовы в случае конфликта с руководством захватить с собой самые значимые для бизнеса базы данных. Речь идет и о системных администраторах, и о топ-менеджерах», – дополняет коммерческий директор компании Agnitum Виталий Янко.

Как признают эксперты, в том, что именно сотрудники становятся ключевой угрозой информационной безопасности, частично виноваты и сами компании. «Когда мы принимаем человека на работу, мы его проверяем. При помощи службы безопасности стараемся на этого сотрудника внимательно посмотреть – кем он был, откуда пришел. Но многие компании останавливаются на этой стадии. Проведя первоначальную проверку, забывают о своих работниках», – рассказывает руководитель технического департамента компании «ОБИТ» Дмитрий Щемелинин. Люди меняются, меняется их отношение к работе, но компании этого не видят.

Но что могут сделать компании, кроме как подписать со всеми сотрудниками соглашения о соблюдении коммерческой тайны? По всей видимости, только одно – довести до максимума принцип разделения полномочий, предельно конкретизировать функции

каждого. «Действительно, большинство угроз исходит изнутри. В частности, в нашей компании в последнее время основной акцент в разработках способов обеспечения безопасности делается на том, чтобы дать человеку как можно меньше информации, но чтобы он мог при этом продолжать выполнять свои обязанности», – делится руководитель отдела информационных технологий компании «Рексофт» Михаил Гусев. Насколько реальны такие инициативы – большой вопрос. Последние десять лет развития российского бизнеса показывают, что в абсолютном большинстве случаев подход к ведению бизнеса противоположный.

Впрочем, не все специалисты согласны с тем, что инсайд – основная угроза для среднего и малого бизнеса. «Страшен не столько уход данных к конкурентам, сколько сама потеря данных, – уверен ИТ-директор компании „Северен-Телеком“ Алексей Григорьев. – Сейчас у малого и среднего бизнеса мало такой информации, которая может стать настоящей бомбой, привести компанию к банкротству. Вот возьмите, например, операторов связи. Что должно в первую очередь привлекать конкурентов? Наша клиентская база. Но не так сложно узнать номерную емкость оператора: просмотрите „Желтые страницы“ и через неделю аналитической работы у вас будет эта клиентская база. С другой стороны, когда собственная клиентская база исчезает, бизнес практически встает. И кстати, надо помнить, что хакерские атаки сегодня нацелены как раз на уничтожение данных».

Эксперты в области безопасности постоянно возвращаются к тому, что обеспечение безопасности – это комплекс разноплановых мер. И из сферы ИТ, и из нормативно-правовой области, и из сферы личных отношений с подчиненными. И подход к обеспечению информационной безопасности также должен сочетать различные оценки – и технических специалистов, и финансовых. Если обобщить то, о чем говорилось на круглом столе, можно выделить следующие четыре пункта, или четыре шага, подытоживает Щемелинин. Первое – определение критически важных активов компании, куда могут входить и технология производства, и бизнес-процессы, и базы данных. Второе – определение возможных мест атаки, откуда исходят угрозы. Это может быть связано с социотехнологическим, то есть человеческим, а может – с чисто технологическим фактором. После этого необходимо определить фактические угрозы, то есть реальные потери. А далее – классифицировать их по степени значимости для бизнеса. И тогда компания приходит к пониманию, стоит ли устранять эти угрозы.