СПЕЦИФИКА ОБЕСПЕЧЕНИЯ IT-БЕЗОПАСНОСТИ В ТЕЛЕКОММУНИКАЦИОННОМ СЕКТОРЕ

Алексей Доля

Выявление специфики защиты информации в телекоммуникационных компаниях позволяет бизнесу построить более эффективную систему IT-безопасности. Однако, чтобы эту специфику выявить, необходимо определить критические для бизнеса компании виды данных, которые необходимо защищать в первую очередь, а потом наиболее опасные угрозы, направленные именно на самую важную информацию. Об этом и пойдет речь в данной статье.

В последнее время отрасль телекоммуникаций становится все ближе и ближе к конечному потребителю. В результате построение эффективной системы IT-безопасности начинает иметь решающее значение для конкурентоспособности телекомов. Фирмы по всему миру стараются укрепить свой бренд, доказав потребителю, что именно они заботятся о своей IT-безопасности больше других, а потому способны предоставлять более качественные услуги. Отметим, что здесь IT-безопасность напрямую связана с качеством, так как инциденты способны вызвать сбои в предоставлении услуг, нарушить непрерывность бизнес-процессов, вызвать простои и больно ударить по карманам – как самой фирмы, так и ее клиентов. В связи с тем, что IT-безопасность так сильно связана с брендом компании, телекоммуникационный бизнес очень чувствителен к инцидентам, способным отрицательно повлиять на имидж и репутацию организации. Между тем, наиболее неприятные последствия в этом отношении вызывает утечка персональных данных клиентов. В результате таких инцидентов пользователи услуг просто отворачиваются от компании, допустившей утечку, и переходят к конкурентам. Кроме того, нельзя сбрасывать со счетов кражу интеллектуальной собственности, так как это один из самых ценных активов любого телекома. От него зависит будущее развитие компании и конкурентоспособность фирмы в ближайшем будущем.

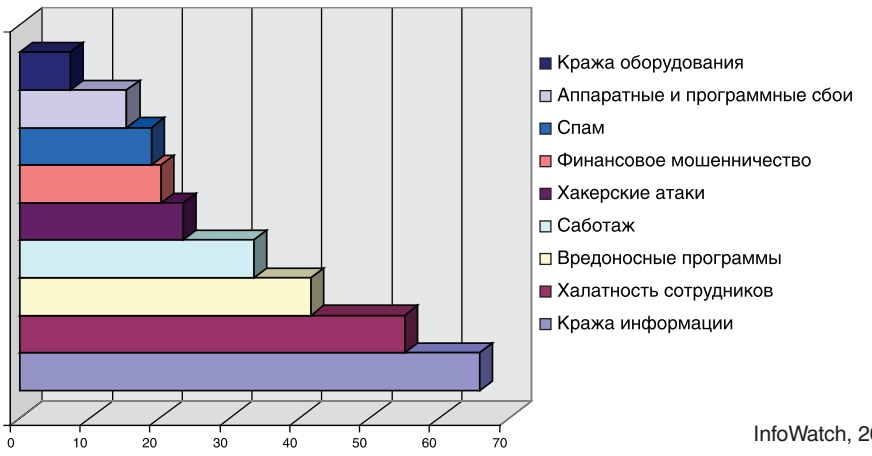
Наиболее опасные угрозы

Обратимся к результатам исследования «Protecting the Digital Assets», которое также известно под названием «The 2006 Technology, Media and Telecommunications Security Survey». В ходе этого проекта компания Deloitte опросила 150 телекомов в более чем 30 странах мира. Респонденты в один голос указали, что наиболее опасная угроза IT-безопасности исходит изнутри компании и направлена она именно против персональных данных клиентов и интеллектуальной собственности предприятия. Другими словами, наибольшую угрозу отрасли представляют инсайдеры или внутренние нарушители, т. е. служащие компании, которые имеют доступ к ценной информации в силу должностных обязанностей и которые могут этим доступом злоупотреблять. Так, 67 % опрошенных телекомов более всего опасаются, что инсайдеры просто отошлют конфиденциальную информацию компании неавторизованным лицам, например, по электронной почте. В то же время 57 % респондентов боятся, что внутренние нарушители станут злоупотреблять корпоративными IT-системами, а 52 % — что инсайдеры украдут интеллектуальную собственность компании.

Посмотрим теперь на российскую статистику. По данным исследования «Внутренние ИТ-угрозы в России 2006», в ходе которого компания InfoWatch опросила 1450 отечественных организаций, включая 274 компании из отрасли телекоммуникаций, наибольший рейтинг опасности приходится именно на внутренние угрозы IT-безопасности: 56,5 % против 43,5 % в пользу инсайдерских рисков. Если же обратиться к структуре на-

Наиболее опасные угрозы IT-безопасности

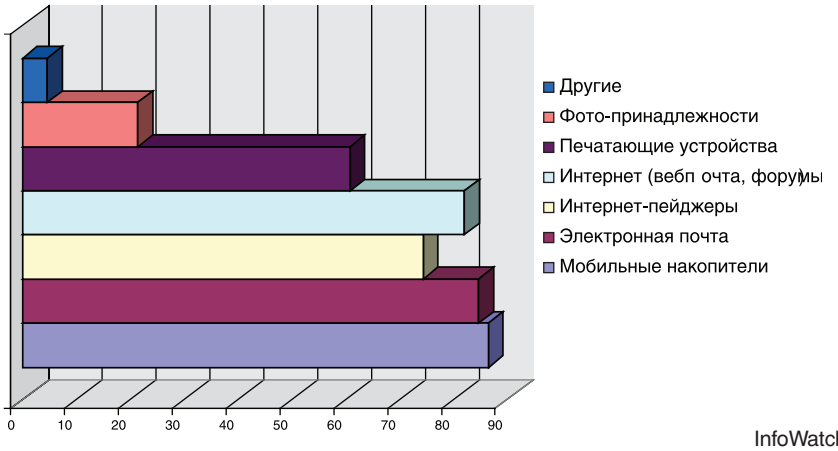
Рис. 1.



InfoWatch, 2007

Наиболее распространенные каналы утечки

Рис. 2.



InfoWatch, 2007

иболее опасных угроз (рис. 1), то на первом месте окажется кража информации (65,8 %), а на втором халатность сотрудников (55,1 %). При этом такие стандартные угрозы, как вирусы (41,7 %), хакерские атаки (23,4 %) и спам (18,9 %) беспокоят российских респондентов далеко не так сильно.

Таким образом, можно утверждать, что наиболее опасные угрозы в секторе телекоммуникаций – это утечка конфиденциальной или приватной информации, а также любые инциденты IT-безопасности, вызванные халатностью сотрудников. Посмотрим теперь, каким образом ценная информация обычно утекает из корпоративной сети. Согласно результатам все того же исследования «Внутренние ИТ-угрозы в России 2006» (рис. 2), наибольшей популярностью среди инсайдеров пользуются мобильные накопители (86,6 %), электронная почта (84,8 %) и Интернет (82,2 %). Другими словами, если компания хочет прекратить утечки из своей сети, ей необходимо в первую очередь закрыть именно эти 3 канала. Однако затем ей также придется сконцентрировать свое внимание и на других путях утечки (рис. 2).

Самая ценная информация

По мнению аналитического центра InfoWatch, наибольшую ценность для телекоммуникационных компаний представляют персональные данные клиентов и интеллектуальная собственность. Причем важность защиты приватной информации существенно возросла после принятия закона «О персональных данных». Остановимся на требованиях этого закона к IT-безопасности, так как в первую очередь эти положения относятся к телекомам.

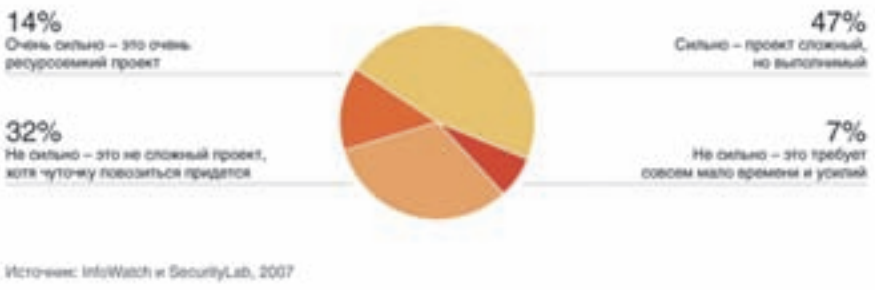
Согласно ч.2 ст.5, «хранение [приватных сведений] должно осуществляться … не дольше, чем этого требуют цели их обработки», а «по достижении целей обработки или утраты необходимости в их достижении» чувствительная информация «подлежит уничтожению». Это означает, что, например, сотовая компания обязана уничтожать персональные сведения своих клиентов, которые отказались от использования ее услуг. Срок, в течение которого уже ставшие ненужными персональные данные должны быть уничтожены, устанавливается ч.4 ст.21 длиной в три рабочих дня. В рамках 7 ст., «операторами и третьими лицами, получающими доступ к персональным данным, должна обеспечиваться конфиденциальность таких данных». Исключений из этого требования всего два: если сведения являются обезличенными или общедоступными, то защищать их не обязательно.

Однако особое внимание представители бизнеса должны уделить ст.19, регулирующей меры по обеспечению безопасности персональных данных при их обработке. Согласно ст.19 ч.1, оператор «обязан принимать необходимые организационные и технические меры, в том числе использовать шифровальные (криптографические) средства, для защиты персональных данных» от целого ряда угроз. Среди них закон выделяет «неправомерный или случайный доступ, уничтожение, изменение, блокирование, копирование, распространение, а также иные неправомерные действия». Другими словами, бизнесу необходимо обеспечить мониторинг всех операций, которые инсайдеры осуществляют с приватными данными клиентов и служащих. Более того, это должен быть активный мониторинг, то есть такой, который позволяет заблокировать действия, нарушающие политику безопасности.

Между тем, реализация всех этих требований в ИТ-инфраструктуре организации наверняка потребует определенных усилий от специалистов компании, а также бюджетных ассигнований на покупку и внедрение новых средств защиты. В связи с этим аналитический центр InfoWatch провел исследование «Защита персональных данных по закону», в ходе которого были опрошены 300 специалистов по IT-безопасности. Одним из вопросов исследования стало выявление того, насколько сильно необходимо модернизировать IT-инфраструктуру организации, чтобы удовлетворить требованиям ФЗ «О персональных данных». Опрос специалистов показал (рис. 3), что большая часть респондентов (47 %) считает этот проект достаточно сложным, но выполнимым.

Насколько сильно придется изменять свою IT-систему в соответствии с ФЗ?

Рис. 3.



При этом IT-систему придется модернизировать довольно сильно. В то же самое время почти треть (32 %) опрошенных профессионалов заявила, что такой проект вряд ли можно считать сложным: сильно менять IT-инфраструктуру не надо, хотя чуточку повозиться все-таки придется. Еще 7% респондентов высказались за то, что это очень легкий проект, а 14% – что очень сложный. Между тем, усредняя ответы, можно сделать вывод, что подавляющее большинство респондентов считает требования ФЗ к защите персональных данных вполне подъемными.

Все данные есть на картинке.

Методы защиты

На основании вышеуказанных исследований Deloitte и InfoWatch можно сделать вывод, что телекомам необходимо защищать персональные данные клиентов и интеллектуальную собственность, причем защищать от утечки и злоупотреблений со стороны внутренних нарушителей. Более того, наиболее часто вся эта информация покидает корпоративную сеть через мобильные накопители и сетевые каналы (Интернет, e-mail), так что их следует взять под контроль в первую очередь.

Между тем, еще одним результатом исследования Deloitte в 2006 году стал тот факт, что хотя многие фирмы отрасли пользуются специальными продуктами, чтобы фильтровать электронную почту, в подавляющем большинстве случаев проверяется лишь входящий трафик (на предмет вирусов, червей и спама). Другими словами, почтовые каналы все еще представляют удобную лазейку для инсайдеров. Хотя многие компании стесняются внедрять системы мониторинга действий служащих, сейчас это совершенно необходимо. Всем фирмам следует, по крайней мере, обеспечить фильтрацию исходящего почтового трафика, а не только входящего. При этом требуется блокировать сообщения, содержащие конфиденциальную информацию и покидающие корпоративную сеть, а не только пассивно выявлять такие письма. Более того, бизнесу необходимо взять под контроль портативные компьютеры, смартфоны и любые другие мобильные устройства, на которых может находиться классифицированная информация в незащищенном виде. Все операции с внешними накопителями должны отслеживаться. Аналитики Deloitte отмечают, что все эти меры могут показаться слишком строгими, но практика показывает, что они достаточно эффективны для защиты ценных данных.

С этим мнением полностью согласны эксперты InfoWatch, а также представители российского бизнеса. По результатам исследования «Внутренние ИТ-угрозы 2006», 44,8 % респондентов признали комплексные IT-решения наиболее эффективным способом борьбы с утечками. Причем 89,1 % компаний планирует внедрить те или иные средства для борьбы с утечками уже в ближайшие 3 года.

Заключение

Угрозы IT-безопасности постоянно растут, развиваются и видоизменяются. Компаниям, работающим в сфере телекоммуникаций, следует отчетливо осознать свою специфику. Эта специфика состоит в том, что защита конфиденциальной и приватной информации в этих компаниях играет решающую роль для конкурентоспособности и сильной торговой марки. Однако важно не только осознать, что именно следует защищать, но и от чего необходимо защищаться. Благодаря неусыпному вниманию прессы, каждая организация наслышана о вирусах, хакерах и нежелательных рассылках. В результате фирмы устанавливают межсетевые экраны и фильтруют входящую почту на вирусы и спам. Однако этого мало, так как сегодня основная опасность исходит изнутри компании. Инсайдеры могут просто-напросто прикрепить конфиденциальный файл к электронному письму и отослать сообщение, куда заблагорассудится. Допускать этого нельзя. Следовательно, требуется обеспечить фильтрацию исходящего трафика и контроль над другими каналами утечки (принтеры, мобильные устройства, съемные носители и доступ к WWW). Это позволит не только защитить интеллектуальную собственность и персональные данные, как таковые, но и предохранить бренд компании от долгосрочных отрицательных последствий утечки.