Е. Г. Кондратова

СОЦИАЛЬНЫЕ СЕТИ КАК КАНАЛ УТЕЧКИ КОРПОРАТИВНОЙ ИНФОРМАЦИИ

В мире современных технологий наиболее успешно развиваются социальные сети, направленные на построение сообществ людей в Интернете со схожими интересами, деятельностью, взглядами на те или иные события. Поэтому, как и любой другой ресурс сети Интернет, социальные сети имеют не только ряд достоинств, но и недостатков, которые влияют как на отдельных лиц, так и на общество в целом. Уже сейчас они представляют собой действующий инструмент информационного влияния, в том числе в целях манипулирования личностью, социальными группами и обществом в целом, а также поле информационных войн [1].

Безусловно, самым простым выходом из сложившейся ситуации является полный отказ от пользования социальными сетями, но на данном этапе развития общества это невозможно. Поэтому каждому следует задуматься о правильном поведении в социальных сетях, изучать необходимую документацию по ИБ, а также следить за новостями по рассматриваемой тематике [2].

В настоящее время можно выделить несколько потенциальных угроз ИБ организации при использовании социальных сетей [3]:

1. Инсайдерские атаки, в том числе социальная инженерия;
2. Компрометация данных сотрудником организации (умышленно, неумышленно);
3. Вирусы, шпионы, спам, фишинг.

Стоит отметить, что владельцы социальной сети не несут ответственности за персональные данные пользователя, а также за распространение и удаление размещенной информации, что указано в пользовательском соглашении. Соответственно, действие Федерального закона «О персональных данных» не распространяется на нее [4]. Поэтому следует четко понимать, что вся ответственность лежит на пользователях интернет-ресурса.

Для корпоративной ИБ существует ряд мер защиты от утечки данных, начинающихся с построения системы управления ИБ, анализа и оценки рисков, выявления наиболее ценной информации и активов, с последующим моделированием убытков, вызванных утечкой информации, а также выявлением и разработкой оптимальных мер по защите. Чаще всего их подразделяют на инженерно-технические — комплексные средства мониторинга, анализа и фильтрации входящего и исходящего трафика на уровне шлюзов, а также средства анализа поведения приложений и сетевых коммуникаций, и организационные — управление доступом к потенциально опасной среде, т. е. диверсифицированные внутрикорпоративные политики «белых списков» и фильтрации контента для различных групп пользователей. Еще один важный аспект, который следует учитывать, — человеческий фактор, поэтому следует принимать методы по усилению рабочей дисциплины, корпоративной этики, а также доносить до сотрудников понимание, что политика ИБ служит не для вторжения в их частную жизнь и ущемления достоинств или прав, а мерой предотвращения потерь и утечки данных компании, особенно если речь идет об информации ограниченного доступа. Следует проводить такие мероприятия, как тренинги и обучение персонала, в том числе риторике и деловому общению, что демонстрирует заинтересованность работодателя в повышении мер защиты информации [5].

Стоит еще раз отметить, что проблемы утечки информации грозят репутации компании, причем доверие клиентов, как показывает практика, равносильно деньгам. Не важно, каким образом компания решает взаимодействовать с таким явлением, как социальная сеть, важно, чтобы были разработаны стратегия решения проблем утечки данных и политика ИБ компании.

СПИСОК ЛИТЕРАТУРЫ:

1. *Губанов Д. А., Новиков Д. А., Чхартишвили А. Г.* Социальные сети: модели информационного влияния, управления и противоборства / Под ред. чл.-корр. РАН Д. А. Новикова. М.: Издательство физико-математической литературы, 2010. — 228 с.
2. Доктрина информационной безопасности Российской Федерации.
3. Аналитика фишинговых атак [Электронный ресурс]. URL: http://www.securelist.com/ru/analysis (дата обращения: 15.01.2013).
4. Федеральный Закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных».
5. Журнал «Information Security/ Информационная безопасность» [Электронный ресурс]. URL: http://www.itsec.ru (дата обращения: 18.01.2013).

А. М. Коротин, П. В. Смирнов

РЕАЛИЗАЦИЯ СРЕДСТВА ПРОЗРАЧНОГО ШИФРОВАНИЯ ФАЙЛОВ НА БАЗЕ СЕРТИФИЦИРОВАННОГО СКЗИ ДЛЯ ОПЕРАЦИОННОЙ СИСТЕМЫ LINUX

В настоящее время одним из решений задачи обеспечения конфиденциальности информации, хранящейся в файловой системе, является шифрование. Существуют различные методы и способы шифрования. Например, пользователь может зашифровать свои файлы и хранить их в защищенном виде. При необходимости использования этих файлов пользователь должен расшифровать их, провести с ними нужные ему операции и затем снова их зашифровать. Неудобство данного способа шифрования состоит в том, что при каждом обращении к файлам пользователь должен сам расшифровывать, а затем зашифровывать их. Для него было бы гораздо удобнее, если бы система сама производила данные операции.

Прозрачное шифрование, известное также как шифрование в режиме реального времени, является методом шифрования, при котором данные зашифровываются и расшифровываются без участия пользователя с помощью драйвера, работающего в фоновом режиме и следящего за всеми обращениями к данным [1]. Основной целью этого метода шифрования является защита от атак, направленных на получение данных в обход операционной системы, т. е. путем загрузки через другую ОС или использования средства прямого доступа к жесткому диску.

На данный момент существует большое разнообразие средств прозрачного шифрования файлов на диске. Практически все они используют иностранные криптографические алгоритмы. Согласно перечню средств защиты информации, сертифицированных ФСБ России, по состоянию на 20 сентября 2012 г. [2], сертифицированные средства прозрачного шифрования существуют только для операционной системы Windows (например, КриптоПро CSP 3.6.1 [3]). Для операционной системы Linux на сегодняшний день таких средств нет. Начиная со сборки ядра 2.6.19, для осуществления технологии прозрачного шифрования используется шифрующая файловая система eCryptfs. Наиболее перспективным представляется внедрение российских криптографических алгоритмов в уже существующее и работающее средство, каким является eCryptfs. Аналогичным образом было спроектировано средство прозрачного шифрования КриптоПро EFS для ОС Windows [4], которое, по сути, является надстройкой над файловой системой EFS с набором дополнительно поддерживаемых функций, таких как контроль целостности информации.

Данная работа является продолжением исследований, которые были представлены в статье «О способах реализации прозрачного шифрования файлов на базе сертифицированного СКЗИ