Ксения Шудрова, shudrova.blogspot.ru

Химеры информационной безопасности

Каждый специалист по защите информации рано или поздно задумывается о границах своих возможностей. В данной статье мне хотелось бы порассуждать о том, что является неосуществимым на данный момент, спустя пару лет мы с вами будем наблюдать совсем другую картину и причин тому масса: глобализация, изменение потребностей бизнеса, увеличение мощности информационных систем и многое другое.

Химера № 1 «Каждая организация занимается вопросами защиты информации».

Безусловно, это то к чему нужно стремиться и я верю, что когда-нибудь защита информации будет такой же повседневной задачей, как охрана труда и пожарная безопасность. Однако на сегодняшний день позволить себе иметь в штате специалиста по информационной безопасности могут далеко не все, это скорее исключение, чем норма. Современная экономическая ситуация не позволяет делать оптимистических прогнозов о значительном увеличении рабочих мест в отрасли, поэтому будет сохраняться тенденция совмещения обязанностей специалиста по информационной безопасности существующим штатным специалистом (из ИТ-отдела, либо Службы безопасности). Часто можно видеть вакансии системного администратора-безопасника, специалиста по собственной и информационной безопасности, специалиста по экономической и информационной безопасности и многие другие варианты.

Все организации условно можно разделить на три категории:

- Организация, в штате которой находится специалист по защите информации (отдел, служба, управление по ИБ) и/или организация пользуется услугами аутсорсинговых компаний в этой области – крупные промышленные предприятия, банки, университеты;
- Организация, в которой функции защиты информации возложены на сотрудника, занимающегося иными задачами (чаще всего ИТ, СБ, однако мне приходилось видеть кадровиков, в обязанности которых входит защита персональных данных) – школы, небольшие конструкторские бюро, рекламные агентства, сети магазинов;
- Организации, не занимающиеся защитой информации – небольшие организации, оказывающие услуги населению, некоторые больницы, маленькие магазины, управляющие компании.

Организация может свободно перемещаться из одной категории в другую, в зависимости от своего текущего финансового положения. Можно отметить, что защите информации уделяется все больше внимания, однако стопроцентный охват всех существующих юридических лиц в России – это пока химера.

Химера № 2 «Нормативно-правовые акты в области информационной безопасности не вступают в противоречия друг с другом, а также в них содержатся точные рекомендации для каждого конкретного случая».

Достаточно вспомнить ФЗ «О персональных данных», это как раз тот случай, когда «два юриста – три мнения». Можно отметить, что последние уточняющие документы внесли определенную гармонию в этот вопрос, однако, точно ответить на вопрос – «Что делать оператору?» не берется никто. Кроме этого можно привести в качестве примера понятие «конфиденциальная информация», данный термин никак не определен в нормативно-правовых актах, однако, при желании вы можете получить лицензию на техническую защиту конфиденциальной информации. Можно сказать, что ситуация постепенно улучшается, но споры по поводу различного понимания одних и тех же статей законов, будут идти еще очень долго.

Химера № 3 «Современные средства защиты информации позволяют обнаружить все каналы утечки информации».

Данное утверждение можно встретить в рекламных буклетах, особенно это касается DLP-систем. Красочные картинки, которыми пестрят их презентации, упорно доказывают нам, что сотрудники для осуществления своих коварных планов используют лишь разрешенные каналы передачи информации. До тех пор, пока мы не научимся стирать память на выходе из территории предприятия, риск утечки информации будет актуальным. Но нужны ли нам сотрудники, которые каждый день будут начинать с чистой страницы, забыв все, что делали вчера?

Химера № 4 «Использование комплекса сертифицированных средств защиты информации обеспечивает абсолютную безопасность информационной системы».

Этот пункт можно считать аналогичным предыдущему. Но мне хотелось бы выделить его отдельно. До сих пор среди специалистов, особенно недавних выпускников, распространено поклонение сертифицированным средствам защиты. Безусловно, существуют такие направления, как защита государственной тайны, здесь мы не можем экономить, и обязаны установить проверенные средства определенного класса защиты, однако, для защиты коммерческой тайны таких требований нет. Мы можем видеть на сайте производителя две цены – за сертифицированную и обычную версии, они различаются весьма значительно. Сертификат – это по большей части формальность (да простят меня интеграторы) и как уже было указано выше, существует человеческий фактор – важная информация может быть переписана, запомнена, сфотографирована на мобильный телефон.

Химера № 5 «Пользователи соблюдают требования информационной безопасности».

Как бы мы не хотели, сколько бы инструктажей не проводили – сотрудники и клиенты будут нарушать требования информационной безопасности. Причин тому множество: лень, занятость, непонимание сути правил, а иногда и невозможность их выполнить. Можно сколько угодно ругать руководителя структурного подразделения за то, что важные документы выбрасываются в мусорные корзины, а не уничтожаются, но для начала неплохо было бы выделить деньги на закупку шредеров. Пишут правила и выполняют их – разные люди. Контролировать клиентов очень тяжело, как с технической, так и с организационной точки зрения. С сотрудниками дело обстоит проще – по крайней мере, существует множество средств контроля, которые можно установить на служебные компьютеры. Не всегда при разработке требований учитывается специфика работы сотрудников, выбирая между тем, чтобы соблюсти рекомендации специалиста по ИБ и поручения своего непосредственного руководства, как вы думаете, что они выберут?

Целью данной статьи было размышление о неразрешимых пока проблемах информационной безопасности, безусловно, это неполный список. Можно еще упомянуть о ключах шифрования и стойкости паролей, а также о безуспешном противодействии методам социальной инженерии. У каждого специалиста есть свой список «химер», какие-то из них глобальные, другие не разрешимы только в пределах одной организации. Понимание уязвимых мест защиты позволит создать принципиально новые технологии, лишенные недостатков их предшественников и завтра мы еще чуть-чуть приблизимся к идеалу абсолютной безопасности.