Почему кибербезопасность юридической фирмы – задача юристов, а не айтишников?

11.07.2016 СТАТЬИ

Хольгер Цшайге, генеральный директор «Инфотропик медиа»

Прежде, чем ответить на этот вопрос, определим понятие «кибербезопасность». Это комплексная система защиты ИТ-инфраструктуры и находящихся в ней данных от внешних и внутренних атак. Слово «комплексная» означает, что система защиты состоит из многих частей, и они все нужны. Своевременного обновления антивируса и блокировки сомнительных сайтов на офисных компьютерах недостаточно.

Если речь идет о безопасности ИТ-инфраструктуры, то почему за это отвечают юристы? Вы же наняли для этого специалистов. Все правильно, только эти специалисты работают на вас, а не вы на них. Соответственно они выполняют поставленные вами задачи в рамках выделенного бюджета. Для корпоратива вы выбираете креветки, а не крабовые палочки, чтобы партнеры не лежали потом две недели в больнице с пищевым отравлением. А на безопасности компьютеров и данных вы стараетесь сэкономить. Хотя по данным Gartner,

40% фирм, у которых случилась серьёзная проблема ИТ-инфраструктуры, ушли из бизнеса в течение года.

Другими словами, ваши данные — ваша ответственность. Потеря данных – это потеря репутации. А хорошая репутация для юридической фирмы — это как справка санэпидемстанции для чебуречной. Поэтому именно юристы должны задавать тон, когда речь идет о безопасности данных.

Вполне возможно, что вы думаете, что находитесь в полной безопасности. Как врачи считают, что здоровых людей нет, есть недообследованные, так и хакеры уверены, что всегда есть брешь в системе защиты. И эта брешь не всегда в компьютере. Рассмотрим несколько примеров из жизни.

1. Хакер, который хочет атаковать вашу систему, изготавливает несколько десятков красивых флеш-накопителей с вредоносной программой и раскидывает их на пути ваших сотрудников в офис. Одну из них обязательно возьмет его (халява же) и поставит в USB-разъем своего компьютера. Voila, ворота в вашу систему открыты. Так иранцы потеряли 10 000 центрифуг для обогащения урана.

2. Ваша бухгалтерия получает письмо от «Комуса» о неоплате счета и просьбой проверить. PDF или картинка счета прилагается. Бухгалтер открыл файл, и все данные в вашей компьютерной сети зашифровали. Для разблокировки требуют заплатить 10 биткоинов. При этом бухгалтер уверен, что письмо пришло от «Комуса». Он в жизни не слышал о header spoofing, да и вы не слышали. Американцы в прошлом году платили 325 миллионов долларов США только одной группе кибервымогателей, работающих по такой схеме.

3. Ваш сайт работает на распространенном «движке» (WordPress, Joomla, и т.д.) и не обслуживается профессионалами. Рано или поздно на нем появятся скрытые для обычного посетителя страницы с рекламными текстами и ссылками на сомнительные

ресурсы (вставленные благодаря дыркам в коде, которые вы не залатали). Вы их не заметите, но Google и Яндекс заметят и постепенно снизят рэнкинг вашего сайта. Вскоре вас не найдут в поисковиках, поскольку те думают, что вы предлагаете не юридические услуги, а препараты для борьбы с эректильной дисфункцией.

4. Ваш сотрудник скачал прикольную игру на свой служебный смартфон на базе Android. О том, что эта программа сливает все ваши данные на сервер в Китае, вы никогда не узнаете. При установке программ на смартфон вы анализируете, какие права доступа запрашивает программа? Не спрашивали себя, зачем программе «Фонарик» нужен доступ к вашей адресной книге и к интернету?

Если все так плохо, и хакеры всегда на 3 шага впереди, то зачем ломать голову о кибербезопасности? Во-первых, хакеры — тоже люди и идут по пути наименьшего сопротивления. Зачем они будут тратить несколько дней на взлом хорошо защищенной системы, если за это время можно взломать 10 других? Во-вторых, угроза от хакеров – не единственная опасность. Сотрудник может «слить» базу клиентов перед уходом к конкурентам. Секретарь на ресепшн ответит «Да» на вопрос системы: «Удалить все файлы?». Аккумулятор ноутбука воспламенится при зарядке и превратит ваш ноутбук в кусок угля. Список можно продолжить на несколько страниц.

Чтобы крепко спать по ночам, вам нужен план на день X. Когда вас атаковали, когда не туда нажали или когда охранник забыл выключить электроплиту и весь бизнес-центр сгорел. Иначе для вашей фирмы не будет дня Y.

14 сентября журнал «Legal Insight» и ФРИИ проводят первую конференцию в России про кибербезопасность для юристов. Чтобы понять статус кво в юридических фирмах, мы проводим опрос. Примите участие в опросе, и мы с вами вместе улучшим безопасность ваших данных! **Всем участникам опроса – скидка на участие в конференции**.

СТАТЬИ