Разоблачения Сноудена расходятся кругами по воде. США, ЕС, Россия, Китай, Латинская Америка втянуты если не в самую разоблачительную, то уж точно в самую захватывающую шпионскую интригу десятилетия. Политики обмениваются взаимными обвинениями, дипломаты – оправданиями, спецслужбы еще больше, чем это вообще возможно, затаились. А простые граждане пока лишь с интересом наблюдают: большинству кажется, что это все не про них и не имеет никакого отношения к повседневной жизни обычного человека. На самом же деле этот скандал – еще один повод задуматься о личной кибербезопасности каждого.

Информация о киберпреступлениях появляется в новостях почти ежедневно, и разнообразие их просто поражает: от многочисленных бытовых хищений денег с пластиковых карт до рассылки ложных писем с информацией об отставке главы РЖД Владимира Якунина.

Кроме морального вреда – удара по репутации, ущерба для деловых партнеров, виртуальные противоправные действия могут нанести вполне реальный денежный ущерб.

Меньше месяца назад спецслужбы Великобритании и США записали на свой счет (в этом случае совместный) раскрытие и ликвидацию группы киберпреступников, которая похитила с карточных счетов кредитные средства банковских клиентов в размере около 200 млн долл. За 2007–2013 годы мошенники смогли получить доступ к данным более чем миллиона кредитных карточек посредством взлома сайтов интернет-магазинов и перепродали их «заказчикам», которые потом использовали эту информацию для несанкционированного доступа и неправомерного списания средств. По оценке различных правоохранительных органов, всего в 2012 году киберпреступники смогли похитить 13 млрд долл., а в этом году, по мнению экспертов, сумма как минимум удвоится.

Тем временем недавнее исследование HarrisInteractive, проведенное по заказу компании Impermium, которая специализируется на защите учетных записей от кибервзлома, наглядно демонстрирует, что одна из самых технологически продвинутых наций – американская – весьма индифферентно относится к личной кибербезопасности. Хотя 79% респондентов обеспокоены, что их e-mail может быть скомпрометирован, 71% переживают, что банковский счет может быть взломан, а 55% волнуются за учетные записи в социальных сетях, три четверти никогда не используют двухфакторную

аутентификацию для защиты своих онлайн-данных.

Как ни странно, одна из причин отказа от дополнительных мер безопасности – изначальное недоверие к самим компаниям и сайтам, ведь в случае с некоторыми способами двухфакторной идентификации пользователям сначала нужно поделиться, например, номером мобильного телефона, на который потом приходят пароли. В итоге получается замкнутый круг: отказывая компаниям и сайтам в доверии, клиенты фактически добровольно отказываются от собственной безопасности.

Новые возможности всегда несут новые риски. Вопрос в соотношении и разумном использовании. На всех уровнях – от государственного до личного – каждому приходится искать наиболее безопасное и выгодное сочетание пользы и защищенности. Причем не стоит думать, что правительства и бизнес используют свои возможности лишь в собственных целях. Государства делают многое для защиты своих граждан во всех сферах. Виртуальная реальность уже охвачена законодательством, которое гарантирует приватность, безопасность, обеспечение всех реальных прав и свобод.

Частные компании также прекрасно понимают, что лучший клиент – это клиент, который доверяет. Чтобы заслужить это доверие, бизнес тратит миллиарды на развитие технологий, призванных повысить уровень надежности и защиты. Кроме собственно технологических разработок многие уже давно прибегают и к другим решениям, направленным на минимизацию ущерба в случае возможных проблем.

Одно из таких решений – комплексное страхование рисков, возникающих при самых различных проблемах: от направленных взломов до потери рабочих ноутбуков, от распространения вируса до сознательного внутреннего вредительства. Кроме компенсации непосредственных убытков – утерянных денежных средств, рабочего времени на восстановление нормального режима работы, выплат клиентам за возможный моральный ущерб, компании также могут воспользоваться возможностями привлечения сторонних консультантов для минимизации последствий киберинцидента.

Продукт распространяется на самые необходимые и жизненно важные риски: сбои в работе корпоративной системы, хищение или потерю информации, компьютерные атаки и распространение вирусов. Компенсация включает также затраты на юридические консультации и представительство в связи с возможным расследованием, расходы на восстановление репутации. Страхование киберрисков также предоставляет

возможность дополнительно включить в покрытие страховые случаи, связанные с нарушением авторского права, плагиатом, неверным освещением и публичным раскрытием информации. А в партнерстве с ведущими юридическими и PR-фирмами и компаниями по электронной безопасности продукт обеспечивает всестороннюю консультационную поддержку.

Выбор же в итоге каждый делает для себя сам – разумное использование имеющихся возможностей почти гарантированно убережет если не от возможного вреда, то от его последствий.

Источник: РБК daily , 18.07.13

Автор: Владимир Кремер, руководитель отдела страхования финансовых рисков ЗАО «АИГ»