Прогноз рисков для британских юристов на 2016-2017 гг.: рост киберпреступности

29.08.2016 СТАТЬИ

Алиса Графтон, *партнер CHEESWRIGHTS*

В конце июля этого года новое правительство Великобритании, возглавляемое Терезой Мэй, буквально в последнюю минуту приостановило подписание долгожданного и жизненно необходимого для Соединенного Королевства договора с французской коммунально-энергетической компанией EdF о строительстве атомной энергетической станции на юге Англии. Часть инвестиций в совместном предприятии по постройке АЭС фактически принадлежит Китаю. Это заставило Терезу Мэй взять тайм-аут и серьезно задуматься о возможных последствиях данного обстоятельства для национальной безопасности. Власти Великобритании опасаются такого активного участия иностранного государства в стратегически важном национальном проекте промышленной инфраструктуры. В связи с этим в прессе не утихают дебаты в отношение репутации «китайских» хакеров. В свою очередь, схожая репутация российских «киберзлодеев» легла в основу версии российского следа в кибератаке на Демократический национальный комитет США, совершенной накануне заключения конвенции демократов. Подтвердятся ли данные обвинения, покажет будущее, но во избежание повторения инцидента демократы уже объявили о создании консультативного совета по кибербезопасности.

Юридическая сфера, так же как стратегическая национальная инфраструктура и политика, представляет собой заманчивый объект для киберпреступников. Так, одной из самых громких за последние годы и, увы, не единственной, стала история с панамскими бумагами. Регулятор солиситоров в Англии и Уэльсе (Solicitors Regulation Authority (SRA)), в публикации «Прогноз рисков на 2016/17 гг.» (Risk Outlook 2016/2017) указал на тревожную динамику роста киберпреступлений, существенно осложняющих обеспечение информационной безопасности в юридических фирмах. В частности, были обозначены следующие виды киберпреступлений:

• использование вредоносных программ, в том числе вредоносного программного обеспечения, которое работает как инструмент вымогателя (ransomware);

• социальный инжиниринг (social engineering);

• «мошенничество пятничного вечера» и «мошенничество исполнительного директора» (CEO Fraud).

Вредоносные программы-вирусы существуют фактически с начала широкого использования персональных компьютеров, но в последнее время появляются все более изощренные вариации компьютерного мошенничества. Хакеры, стоящие за ransomware, шифруют файлы и затем требуют выкупа за предоставление ключа дешифровки; при социальном инжиниринге преступники получают конфиденциальную информацию путем завоевания временного доверия ответственного лица в юридической фирме. Социальный инжиниринг также принимает форму «мошенничества пятничного вечера», когда преступники, используя ослабленную в конце трудовой недели бдительность сотрудников юридической фирмы, получают доступ к ее компьютерной системе. Набирает обороты и еще одна форма социального инжиниринга – «мошенничество исполнительного директора», когда киберпреступник, взломав электронный почтовый ящик высокопоставленного лица в юридической фирме или приобретя ящик с исключительно похожим адресом, выдает себя за такое лицо и требует перечисления платежей со счетов данной фирмы.

Актуальной также является проблема фиктивных юридических фирм. По данным SRA, за период с 2012 г. по 2015 г. их число увеличилось вдвое (до 700). Некоторые из них выдают себя за существующие организации, проникнув в их компьютерные системы и используя их электронные адреса для коммуникации с клиентами данной фирмы. Другие прибегают к взлому почтового сервера для перехвата сообщений, содержащих чувствительную информацию, например, такую, как счета фирмы, данные для оплаты которых преступники меняют на фиктивные, прежде чем перенаправить их якобы с сервера данной фирмы существующим клиентам для оплаты.

Проблема кибербезопасности в юридическом мире не имеет государственных границ, ее актуальность сложно переоценить как для английских, так и для российских юристов. Осознавая серьезный риск в отношении одной из основных обязанностей юристов – обеспечения конфиденциальности информации, полученной от клиента, – SRA рекомендует:

• принимать разработанные в государственной программе меры по обеспечению кибербезопасности юридических фирм (подробнее об этом говорится в интервью Саймона Шутера

);

• обучать сотрудников минимизации риска, исходящего от социального инжиниринга, фишинга и вишинга (телефонного фишинга);

• своевременно информировать SRA, банки, полицию и страховщиков о случаях, когда клиентский счет подвергается кибератаке.

В преддверии конференции по кибербезопасности для юристов Алиса Графтон побеседовала С аймоном Шутером, партнером лондонского офиса юридической фирмы Bird & Bird, об эффективной системе защиты от киберпреступлений, задачах, стоящих перед юристами, партнерами и менеджерами юридических фирм, и путях их решения в мире современных технологий.

Статья опубликована в Legal Insight №7. 2016.

Читайте также:

СТАТЬИ