

В 2017 г. у компаний, работающих с персональными данными россиян, есть два повода для беспокойства. Первый – очевидно возросший уровень киберугроз. Недавняя атака вируса-вымогателя Petya в очередной раз продемонстрировала, что чувствовать себя в полной безопасности сегодня не может никто. Второй – усиленное регулирование сферы персональных данных со стороны законодателей и регуляторов (с 2018 г. операторам связи придется хранить большие массивы персональных данных, а значит, и защищать их). Рост административного контроля вынуждает бизнес дополнять борьбу с рисками инструментами страхования.

Снаряд и броня

Работа с киберугрозами развивается по классическому сценарию, хорошо знакомому оружейным инженерам. Есть партия обороны – она работает с броней и рубежами защиты, и есть партия нападения – хакеры, системы промышленного шпионажа, террористы. Для бизнеса – банков, систем продаж авиабилетов, сотовых операторов и др. – этот сценарий приводит к постоянному росту расходов на «гонку вооружений». И, как на настоящей войне, эти траты не гарантируют от потерь.

На сегодня, по данным AIG, средняя стоимость одного инцидента с хищением данных в мире не превышает $4 млн. В финансовом секторе эта цифра доходит до $14 млн, в энергетике – около $10 млн. На российском рынке эти цифры отличаются не сильно: по данным Group IB, максимальная сумма хищения хакерами у российского банка в 2016 г. составила 600 млн руб. ($9 млн). При этом в другом крупном банке была предотвращена попытка хищения 1 млрд руб. ($16 млн).

Основные убытки пострадавшие от взломов и утечек компании несут по двум направлениям: перерывы в работе (а если это, например, авиакомпания, то убытки могут исчисляться миллионами долларов) и компенсации пострадавшим клиентам, чьи персональные данные были украдены.

По статистике «Лаборатории Касперского», в 2016 г. 42% российских компаний хотя бы один раз теряли важную информацию из-за взломов или утечек данных. Треть компаний-клиентов обратились к ее услугам, потому что это случалось неоднократно.

Слабым утешением служит то, что, несмотря на постоянный рост с 2015 г. попыток кибератак, ежегодный ущерб от них, нанесенный, в частности, российским финансовым компаниям, снизился почти в четыре раза. Это связано с тем, что одними из главных каналов утечек конфиденциальной информации являются не внутренние системы и серверы, а браузеры клиентов и облачные хранилища. В последние годы в фокусе хакеров частные лица: они гораздо более легкая добыча для преступников, нежели крупные компании. Все чаще преступники получают доступ к электронным кошелькам и системам онлайн-банкинга, подключенным к телефонам, смартфонам и планшетам, – это позволяет красть средства и информацию граждан и получать доступ к информационным системам компаний и банков.

За чей счет атака

Недавний опрос, проведенный AIG среди руководителей американских компаний, переживших успешные кибератаки, показал, что каждый третий топ-менеджер предпочитает не вкладывать деньги в разработку дополнительных средств защиты информации (используют готовые решения), а просто страховать такие риски. Если возможные потери могут быть измерены в деньгах, то выгоднее страховать риск, а не постоянно наращивать бюджет «гонки вооружений».

Этот подход можно представить в виде простой математической задачи. Если грабителю с пистолетом в банке интересны один-два входа в конкретном отделении и два-три места хранения наличных, то количество виртуальных целей злоумышленника в одной информационной системе и способов доступа к ним может исчисляться десятками. В результате IT-специалисты играют в игру со многими неизвестными, и это множество не конечно.

В России сейчас действующих комплексных полисов по страхованию киберрисков сравнительно немного. Но чем глубже бизнес-процессы будут погружаться в онлайн-среду, тем более востребован будет этот продукт на рынке страхования. Его сложно назвать дорогим: для средних и мелких предприятий стоимость покрытия потерь в размере $1 млн – это $2000-3000. Для крупных финансовых компаний стоимость может доходить до $100 000 премии за $1 млн лимита ответственности страховщика. Но специфика российского рынка в том, что его развитие стимулируют не столько потери от хакеров, сколько административное регулирование.

В 2018 г. сотовые операторы по требованию закона Яровой будут вынуждены хранить огромные массивы персональной информации своих абонентов. К этому времени большинство компаний, работающих с персональными данными (уже несколько лет они должны хранить их на серверах в России), накопят терабайты информации с данными паспортов, номерами кредитных карт, счетов и транзакций. Можно не соглашаться с депутатом Яровой в том, что бороться с терроризмом нужно через архивирование переписки, но отказаться от этого уже нельзя, равно как и защитить данные на 100%. В такой ситуации единственная стратегия – минимизация возможных убытков.

Мнения экспертов банков, финансовых и инвестиционных компаний, представленные в этой рубрике, могут не совпадать с мнением редакции и не являются офертой или рекомендацией к покупке или продаже каких-либо активов.

Источник: Ведомости, 08.08.2017