Несмотря на то что только банковский сектор за последние два года потерял от действий хакеров более 1,5 млрд руб., страхование от киберрисков пока не стало популярным в России. Впрочем, эксперты называют этот сегмент перспективным — имущества в электронном виде становится все больше, с ростом посягательств на него будет развиваться и киберстрахование.

Редкий полис

В 26 млн руб. обошлась «Ингосстраху» хакерская атака на сайт клиента-реестродержателя. Такое возмещение страховщик заплатил акционеру нефтедобывающей компании за хищение акций с помощью вируса: «червь» проник в базы данных регистратора, в результате реальный владелец акций был заменен в базе на другое лицо. «После чего это лицо пришло со своими реальными документами в офис регистратора и на «законных» основаниях выставило пакет акций на продажу»,— рассказал начальник управления страхования ответственности «Ингосстраха» Дмитрий Шишкин.

В данном случае выплату обеспечила нецелевая страховка от кибератак — покрытие риска было оформлено в рамках договора комплексного страхования реестродержателя (регистратора). Покупка отдельного киберполиса на нашем рынке пока еще большая редкость. Киберстрахование обычно продается в качестве опции в комплексном полисе, например, для банка (BBB, Bankers Blanket Bond — страхование банков от преступлений) или для участника рынка ценных бумаг. Киберриски по таким полисам связаны с финансовыми угрозами — это потеря персональных данных клиентов (покрываются расходы на восстановление данных или убытки от их потери), кража денег или акций со счетов клиентов и т. п., рассказывает Дмитрий Шишкин. «Значительный пласт киберрисков — вывод из строя оборудования, организация взрывов, пожаров, ложного срабатывания сигнализаций, когда прибегают к помощи хакеров,— в России недооценивается»,— сокрушается он.

Кибератаки на банки есть и в практике «АльфаСтрахования», но суммы выплат в компании не обнародуют. «Надеемся, что сработавшее страховое покрытие сыграло ключевую роль в том, что убытки банка, возмещенные страховщиком, остались незамеченными ни для прессы, ни для клиентов»,— говорит глава управления страхования финансовых рисков «АльфаСтрахования» Андрей Макаренцев.

В российской практике компании AIG было несколько случаев возмещения ущерба от атак на банки ради кражи денег со счетов, рассказывает руководитель отдела страхования финансовых рисков AIG в России Владимир Кремер. Убытки покрывались по страховке от мошенничества, а выплаты, по его словам, составили «несколько сот тысяч долларов». «Но это только возмещение ущерба от кражи»,— подчеркивает он. Затраты клиента на IT-расследование инцидента и прочие расходы (юридические, PR) покрываются в рамках отдельного полиса по киберрискам, уточнил Кремер.

В западной практике встречаются более крупные выплаты. В отчете международного страхового брокера Willis Towers Watson указывается, что в 2008 году было выплачено $60 млн предприятию финансового сектора в результате взлома данных, что привело к перевыпуску карт покупателей. В 2007 году $40 млн возмещения получило предприятие ритейла, у которого из-за несанкционированного проникновения в систему оказались скомпрометированы номера 45 млн карт клиентов. А в 2011 году хакеры взломали сеть

компании в сфере бытовой электроники, и получили доступ к данным 31 млн пользователей онлайн-игры. Сумма страховки составила $15 млн.
«Наш клиент — сеть универмагов класса люкс — получил уведомление от эмитента кредитных карт о взломе системы, в результате чего были скомпрометированы персональные данные 35 тыс. держателей карт универмага»,— рассказывает о международном опыте AIG Владимир Кремер. Страховая компания потратила $200 тыс. на то, чтобы уведомить держателей и заменить карты, а также на услуги кредитного мониторинга.
Масштаб угрозы
Ежедневно жертвами киберинцидентов в России становятся 16 компаний, которые теряют в день в общей сложности почти 500 тыс. руб.,— эти данные компании Group IB, специализирующейся на расследовании и предотвращении высокотехнологичных преступлений, приводит замдиректора департамента страхования финансовых линий «Альянс» Вадим Михневич. «Расходы на восстановление дееспособности систем составляют $20-60 тыс.»,— добавляет он. В целом в 2016 году ущерб мировой экономики от действий киберпреступников превысил $35 млрд, говорит Андрей Макаренцев.
По данным Group IB, в России ущерб в связи с атаками на банки в 2015-2016 годах составил более 1,5 млрд руб. При этом средняя сумма хищения у юрлица в интернет-банкинге — 480 тыс. руб., а если брать целевые атаки на банк, средняя сумма --140 млн руб. (данные за 2016 год). Большая часть подобных рисков не покрывалась страховкой, поясняют в «Альянсе», так как далеко не все российские банки покупают покрытие ECC (Electronic Computer Crime; спецусловия страхования, которые привязаны к банковской деятельности и касаются умышленных противоправных действий), а отдельные полисы киберрисков вообще не покупают.
Глобальный объем рынка страхования киберрисков оценивается в $2,5 млрд сборов, говорит Вадим Михневич. Причем 80% премий приходится на США — из-за жесткого законодательства и развитой IT-инфраструктуры. Для сравнения: по данным ЦБ, страхование финансовых рисков в целом (киберриски в статистике не выделяются) принесло российским страховщикам 14,4 млрд руб. из 1 трлн руб. сборов в 2015 году.
От киберугроз, как правило, страхуются банки и компании финансового сектора, профучастники рынка ценных бумаг — биржевые регистраторы и депозитарии. В целом необходимость такого полиса признают компании, которые хранят большие объемы персональных данных,— интернет-магазины, компании телекоммуникаций, участники рынка здравоохранения, производственные предприятия, добавляет Вадим Михневич.
Мы чаще сталкиваемся не с киберпреступлениями, а с бытовыми историями — муж по доверенности дал поручение на продажу акций жены, вывел деньги на ее карту и потратил с нее деньги
На медучреждения в мире обрушивается на 340% больше кибератак, чем в среднем на компании других секторов, приводит данные компании Raytheon председатель наблюдательного совета Российского антитеррористического страхового пула Александр Гульченко. «Во-первых, их системы в среднем хуже защищены, так как используют старое оборудование,— объясняет эксперт.— Во-вторых, они хранят ценные сведения: имена, даты рождения, номера страховок, диагнозы, платежную информацию. С помощью этого хакеры могут подделывать документы для покупки и перепродажи лекарств, для обращений по мнимому страховому случаю. На черном рынке США мединформация ценится гораздо дороже, чем номер кредитной карты».

В российской практике законы не стимулируют бизнес страховаться от компьютерных взломов. «Штрафы за нарушение законодательства о персональных данных у нас не так велики, как в Европе и США,— говорит Вадим Михневич.— Например, в Европе штраф доходит до 4% консолидированного оборота компании». В России же штраф для юрлиц составляет 5-10 тыс. руб. (ст. 13.11 КоАП РФ), а нарушение тайны частной жизни (ст. 137 УК РФ) предусматривает штраф до 200 тыс. руб.

Нет в нашей стране и громких случаев с исками к компаниям (например, интернет-магазинам) от клиентов, чьи персональные данные были украдены при взломе, добавляет исполнительный директор, член правления «Согаза» Дмитрий Талаев: «А пока таких случаев нет, нет и осознания важности страхования этих рисков».

Кроме того, непонятно, как будет оцениваться ущерб,— это тоже удерживает наши компании от покупки киберполисов. «По идее у страховщика должен быть полный доступ к данным застрахованного клиента — думаю, что не все готовы его предоставить в полном объеме»,— перечисляет возможные затруднения технический директор холдинга высокотехнологичного кредитования ID Finance Павел Шарейко. Страховщики, с другой стороны, жалуются на ограниченные возможности в расследовании таких случаев, это препятствует урегулированию, считает заместитель главы департамента андеррайтинга СК МАКС Алексей Хуторянский.

Но дело не только в спросе — страховщиков, готовых предоставлять такое покрытие в России, можно пересчитать по пальцам, признает гендиректор страхового общества «Помощь» Александр Локтаев. Причина — недостаток экспертизы: правильно оценить и тарифицировать эти риски под силу лишь крупным СК.

«Для оценки страховой премии и выплат потребуется информация о частоте инцидентов, возможном ущербе, мерах, принятых организацией для минимизации вероятности инцидента и ущерба, об эффективности и оперативности этих мер»,— рассказывает замдиректора по развитию бизнеса Positive Technologies в России Алексей Качалин. Такие данные могут представить лишь эксперты по информационной безопасности.

Даже участники рынка ценных бумаг — целевой сегмент страхования киберрисков — замечают, что страховщики не рвутся их страховать. «Страховщикам не всегда понятны риски профучастников-брокеров. Это сложнее, чем массовые продукты типа каско,— рассуждает основатель интернет-магазина акций Freedom24.ru Дмитрий Панченко.— Мы на тендере получили адекватные предложения только от двух компаний, остальные были очень дорогими и длительными по процедуре».

При этом страховаться имеет смысл комплексно, считает Панченко, а страхование именно от киберугроз сделает покупку акций непривлекательной, так как тарифы страховых компаний высоки. «Мы чаще сталкиваемся не с киберпреступлениями, а с бытовыми историями — муж по доверенности дал поручение на продажу акций жены, вывел деньги на ее карту и потратил с нее деньги»,— рассказывает Дмитрий Панченко. По его словам, Freedom24.ru страхуется от киберугроз тем, что все значимые процессы — переводы ценных бумаг, ввод-вывод денег — замыкает на внутреннвих сотрудников, а также инвестирует в IT.

Эксперты сходятся на том, что рынок страхования киберрисков неизбежно будет расти из-за проникновения технологий и повышения изощренности хакеров. За пять лет рост может быть 2-3-кратным, говорит Вадим Михневич. В России уже появляются программы с покрытием рисков виртуального вымогательства и ущерба деловой

репутации. «Имущества в электронном виде становится все больше — значит, появится и его страхование»,— резюмирует Дмитрий Панченко.

Источник: Деньги, 12.12.2016