

ПРИВИВКА ОТ ВИРУСА

Яна Овсянникова

эксперт ОСАО «Ингосстрах»

Пока разработчики ищут способы борьбы с новыми вирусами, ваш бизнес остается без защиты. Как отмечают эксперты, за всю историю существования Всемирной паутины 2007 г. оказался самым вирусоопасным: число угроз заражения увеличилось более чем в 2 раза. За прошлый год «Лаборатория Касперского» добавила в свои антивирусные базы почти столько же программ, сколько за предшествующие 15 лет. Однако даже самые изощренные разработки не в силах предотвратить убытки компаний от хакерских и вирусных атак. И чем масштабнее электронные преступления, тем чаще организации задумываются о таком способе защиты, как страхование.

ДЕНЬГИ, ИНФОРМАЦИЯ, ОТВЕТСТВЕННОСТЬ

Наиболее известным способом страховой защиты материальных активов от киберугроз является страхование от компьютерных и электронных преступлений. На создание этой услуги страховщиков вдохновили клиенты — финансовые учреждения. В начале 1980-х гг. страховой договор по комплексному страхованию банков (так называемый *Bankers Blanket Bond*, или *BBB*) не учитывал процессы начавшейся компьютеризации. Это, естественно, обеспокоило финансовые институты, стремившиеся максимально обезопасить себя от действий злоумышленников. В ответ на появившийся спрос английский страховой синдикат *Lloyd's* разработал полис от электронных и компьютерных преступлений, который стал частью договора *BBB*.

Инициировав создание полиса, финансовые структуры до сих пор являются главными его покупателями. Как показывает статистика «Ингосстраха», чаще все-

го договор страхования от компьютерных и электронных преступлений заключают банки, биржи, профессиональные участники рынка ценных бумаг. Как правило, полис покрывает риски, связанные с вредом, нанесенным вирусами и вводом подложной информации в электронные базы данных, противоправными действиями сотрудников страхователя. Кроме того, он компенсирует убытки от преднамеренной порчи электронных данных при их хранении, во время записи или при перевозке. Страховщик также возместит потери, возникшие в результате фальсификации документов клиентов и осуществленных на их основании операций и т. д.

Начальник отдела финансовых институтов «Ингосстраха» **Дмитрий Шапошников** отмечает, что сейчас страховой защитой от электронных преступлений все чаще стали интересоваться организации, работающие с информационными активами: базами данных, программным обеспечением и т. п. Они тоже могут пострадать от вирусных и хакерских атак, мо-

шеннических действий, однако убытки по этим активам покрываются уже другим полисом — договором страхования информационных рисков.

Для профессиональных участников рынка ценных бумаг страховое покрытие рисков, связанных с электронными преступлениями, является, помимо насущной необходимости защиты своих ресурсов и систем, также требованием, предъявляемым ПАРТАД для включения этих финансовых институтов в свои члены.

«Применительно к рынку ценных бумаг, в связи с принятием поправок в нормы достаточности собственных средств профессиональных участников рынка ценных бумаг, а также управляющих компаний инвестиционных фондов, паевых инвестиционных фондов и негосударственных пенсионных фондов, договор страхования с включенными в него рисками, связанными с покрытием электронных преступлений, в числе прочих считается ФСФР РФ основанием для снижения норматива достаточности собственных средств профессиональных уча-

стников», — добавляет ведущий специалист отдела страхования финансовых и профессиональных рисков ОСАО «Ингосстрах» Кирилл Свинухов.

Растет спрос и на отдельное направление в сфере страхования информационных рисков — страхование профессиональной ответственности. Такой полис актуален для тех компаний, которые занимаются разработкой, внедрением и обслуживанием программного обеспечения либо оказывают консультационные или аудиторские услуги в сфере информационной безопасности.

«Пока подобный договор заключают только те, кто работает с западными партнерами, требующими от российской компании полис страхования профессиональной ответственности, — говорит Д. Шапошников. — Нередко разработчик программного обеспечения или системный интегратор, оказав услугу клиенту, предоставляет полис профессиональной ответственности как дополнительную гарантию. В любом случае, подобный договор — отличный имиджевый фактор, а также способ восполнить существующие пробелы в сфере ответственности перед клиентом».

В рамках страхования информационных рисков «Ингосстрах» реализует еще одну дополнительную программу — страхование от перерывов в коммерческой деятельности. Как известно, если компания в большой степени зависит от функционирования компьютерных систем, то в случае сбоя ее основная деятельность прекращается и организация несет убытки. Например, для интернет-магазина остановка работы чревата потерями, связанными с недополученной прибылью и текущими расходами. Компенсировать эти убытки поможет полис страхования от перерывов в коммерческой деятельности.

Впрочем, любой из вышеупомянутых видов страхования является лишь дополнительным средством защиты самой компании или ее контрагентов.

Компьютерные вирусы постоянно развиваются: между появлением нового вируса и созданием соответствующей антивирусной программы проходит время. Поэтому, по словам Д. Шапошникова, одна из целей такого страхования — закрыть брешь, которая неизменно возникает в период между разработкой вредоносной программы и рождением нового антивируса.

ОЦЕНИТЬ ВСЕ РИСКИ

Процедура заключения договора в «Ингосстрахе» начинается с заполнения

анкеты. Если компания страхуется впервые, страховщик предлагает ей провести предварительный анализ рискозащищенности — сюрвей. Основная цель страховой экспертизы рисков, осуществляемой независимой российской или зарубежной сюрвейерской организацией, — оценка механизмов управления рисками страхователя и разработка рекомендаций по улучшению его систем безопасности. Благодаря сюрвею клиент получает возможность выявить и «закрыть» слабые места в системах защиты, а страховщик — корректно оценить риск.

Получить верное представление о компании специалистам сюрвейерской организации помогают различные методы. Например, чтобы выяснить, насколько подвержены риску внешнего вторжения извне информационные системы страхователя, проводится так называемый хакинг-тест.

«Сотрудники специализированных компаний, которых можно назвать легальными хакерами, инициируют внешнее внедрение в систему потенциального клиента, — объясняет Д. Шапошников. — Разумеется, их задача не подвесить систему как таковую, чтобы причинить вред компании. Они ищут узкие места, которые позволят третьим лицам, имеющим злой умысел, взломать систему. Несмотря на то что такая процедура не является обязательной при заключении договоров страхования, некоторые российские компании успешно ее прошли».

Что касается информационных активов, то, возможно, потребуется оценка их стоимости. Впрочем, независимо от того, какова будет цена этого актива, страховая выплата будет проводиться по восстановительной стоимости. Как правило, когда обрушивается база данных, остается резервная копия недельной данности. Иначе говоря, чтобы восстановить, например, систему стоимостью 1 млн долл., может потребоваться всего 2 тыс. долл. Однако если по каким-то причинам информационный актив будет утрачен безвозвратно, страховая компания компенсирует полную его стоимость.

Убытки по финансовым активам, например денежным средствам на счетах клиентов, компенсируются в размере реального ущерба. Как раз сейчас в «Ингосстрахе» рассматривается страховой случай, когда в информационной системе банка произошла замена сведений держателя вклада на данные злоумышленника, который впоследствии снял деньги со счета, предъявив свой паспорт.

Как правило, возмещение клиенту выплачивается после того, как в распоряжении страховщика окажется документация, подтверждающая факт наступления страхового случая и его размер. Обычно подобные сведения формируются у клиента после завершения своего внутреннего расследования, однако в ряде случаев для выяснения причин требуется завершение расследования правоохранительных органов. Между тем в «Ингосстрахе» возможна такая ситуация, когда убытки клиента компенсируются до завершения официального следствия.

«IT-эксперты, с которыми мы работаем, могут определить характер вторжения: внешнее либо внутреннее. Можно даже определить, с какого именно компьютера в помещении банка был произведен несанкционированный ввод кодов и паролей», — говорит Д. Шапошников.

БОЛЬШИЕ ЛИМИТЫ СТРАХОВАНИЯ

В «Ингосстрахе» страхование от электронных преступлений в рамках комплексного страхования финансовых институтов развивается уже больше 10 лет. Сегодня у компании есть возможности создать продукт с учетом бюджета клиента, поэтому в каждом случае стоимость полиса будет разной. В целом она зависит от многих факторов, в том числе от размера выбранного лимита ответственности. Например, при лимите 1 млн долл. страховая премия будет колебаться в пределах от 5 до 25 тыс. долл.

Опыт «Ингосстраха» распространяется не только на прямое страхование, но и на перестрахование. Это особенно важно при страховании информационных рисков, профессиональной ответственности и страховании от компьютерных преступлений, когда часто требуется перестраховывать довольно большие лимиты. Находясь в тесном контакте с западными перестраховщиками, в том числе с компаниями, специализирующимися на страховании от электронных преступлений, страховщик может повлиять на ценообразование и снизить стоимость полиса.

Впрочем, если лимит ответственности составляет до 1 млн долл., «Ингосстрах» оставляет риск на собственном удержании. Это сказывается не только на стоимости полиса, но и на скорости выплаты компенсации. Таким образом, если произойдет страховой случай, компания сможет быстро компенсировать убытки и продолжить работу. ■