В последнее время реальной угрозой для бизнеса стали виртуальные атаки. По данным Group IB (компания специализируется на расследовании и предотвращении преступлений в онлайн-сфере), в России в 2015-2016 годах ущерб в связи с атаками на банки составил более 1,5 миллиарда рублей. Сократить потери от виртуального вмешательства в работу компании можно, застраховав себя от киберугрозы. Но к услугам страховщиков на юге России пока прибегает крайне мало компаний.

К примеру, по данным группы компаний "Альфастрахование", к началу сентября 2017 года совокупная сумма страхования, предоставленного корпоративным клиентам по этому направлению, превысила 100 миллионов евро. Всего под защитой страховщика сейчас более 20 крупных российских предприятий, и только два из них зарегистрированы в ЮФО. Еще несколько южных компаний проявили интерес к таким продуктам, и сейчас страховщики ведут с ними переговоры.

— Общий ущерб мировой экономике от киберпреступлений за прошлый год превысил 35 миллиардов долларов, — говорит глава управления страхования финансовых рисков "Альфастрахование" Андрей Макаренцев. — От киберугроз, как правило, страхуются банки и компании финансового сектора, профучастники рынка ценных бумаг — биржевые регистраторы и депозитарии. Полис также пригодится компаниям, оперирующим большим объемом информации: ретейлу, телекоммуникационным, участникам рынка здравоохранения и производственным предприятиям.

Сегодня страхуемые угрозы можно условно разделить на три группы. Первая — это гражданская ответственность за утрату персональных и финансовых данных клиентов. Здесь речь идет о возмещении вреда по требованиям, которые могут предъявить компании при утечке или раскрытии такой конфиденциальной информации. Вторая категория касается остановки производства и убытков в связи с этим: потеря чистой прибыли и расходы на продолжение деятельности компании в условиях кибератаки. И третья категория — расходы на расследование подобных инцидентов и помощь со стороны специалистов.

Сказать, сколько стоит в среднем такой киберполис, невозможно, так как страхование от виртуальной угрозы — дело индивидуальное. Эксперты говорят, что, прежде всего, нужно провести технический аудит, который позволит оценить, в каком состоянии находится IT-система компании. Важно и то, чем занимается потенциальный страхователь. Так, электронная служба заказа такси на сто процентов зависит от благополучия ее IT-системы. Риск здесь высок, значит, и полис будет дороже. А в небольшой компании, к примеру, в сфере ЖКХ, опасность уже не столь велика.

— Вывод из строя оборудования в результате хакерской атаки, взрывы, пожары, ложное срабатывание сигнализации из-за взлома систем безопасности через внешний доступ пока недооценивается нашими клиентами, хотя мы уже видим примеры, когда наличие такого полиса могло бы помочь возместить ущерб и спасти от гибели

промышленное предприятие, — говорит Андрей Макаренцев.
По мнению участников рынка, недостаточная активность потенциальных страхователей связана отчасти с тем, что этот риск российские компании пока недооценивают, а отчасти с нежеланием тратить достаточно большие суммы на гипотетическую атаку, которая то ли будет, то ли нет.
И тем не менее страховщики и аналитики полагают, что уже в ближайшие годы картина будет меняться. Донской эксперт в области финансового планирования и инвестиций Игорь Захидов считает, что страховые компании, обратившие внимание на такой продукт уже сегодня, обязательно окажутся в выигрыше, так как буквально через три-пять лет страхование киберриска будет достаточно распространено.
— Более того, я думаю, что застраховать себя от хакерской атаки захотят не только крупные корпоративные клиенты, но и обычные граждане, которые являются активными пользователями. Мы все больше уходим в Сеть, совершаем огромное количество электронных транзакций и хотим быть застрахованными от виртуальной угрозы, — уверен Захидов.
Между тем
Специалисты страховой компании Allianz накануне запуска нового продукта по страхованию киберугрозы провели опрос, чтобы выяснить, насколько же защищены сегодня российские предприятия и предприниматели. Участие в исследовании приняли более 120 крупнейших российских и международных компаний. Оказалось, что 67 процентов компаний не готовы к потенциальной кибератаке, а 53 процента — либо не имеют антикризисного плана действий в этом случае, либо имеют его исключительно на бумаге.

Источник: Российская газета, 26.09.2017