РБК+

ТЕМАТИЧЕСКОЕ ПРИЛОЖЕНИЕ К ЕЖЕДНЕВНОЙ ДЕЛОВОЙ ГАЗЕТЕ РБК

Четверг, 27 октября 2022 | № 133 (3626)

Информационные технологии

ТЕНДЕНЦИИ | Как бизнес перестал экономить на безопасности

На фоне роста угроз и более осознанного подхода компаний к вопросам информационной безопасности рынок ожидает увеличения спроса на услугу киберстрахования.

Бизнес начал вкладывать в страхование киберрисков

Фото: Getty Images Russia

ДАРЬЯ АРДЖЕНТОВА

Бизнес озадачен защитой своих информационных систем. В 2022 году число кибератак и попыток их совершения существенно выросло, отмечают эксперты. С конца февраля изменился ландшафт атак, отмечает руководитель направления аналитики киберугроз компании «РТК-Солар» Дарья Кошкина. «От массовых DDoS- и веб-атак злоумышленники перешли к более сложным и точечным ударам. Преимущественно эти атаки связаны с заражением вредоносным ПО — во втором полугодии 2022 года на них пришлось почти 30% зафиксированных нами инцидентов. То есть в первые месяцы года хакеры усиленно и, можно сказать, бездумно «бомбили», теперь же развивают атаки там, где удалось проникнуть внутрь», — уточняет Дарья Кошкина.

Главный технологический эксперт «Лаборатории Касперского» Александр Гостев также отмечает агрессивность атак на российские организации. Все чаще, по его словам, злоумышленники нацелены не на получение выгоды, а на то, чтобы нанести максимальный ущерб и нарушить процессы. Особенно опасно это для объектов критической инфраструктуры и промышленности.

На фоне увеличения числа угроз и их сложности можно ожидать повышения спроса на комплексные защитные решения и страхование киберрисков, полагает Александр Гостев. Тем не менее в России такая услуга все еще остается нишевым продуктом, не имеющим массового потребителя, считает директор департамента андеррайтинга и перестрахования компании «Абсолют Страхование» Евгений Ильченко. «С развитием цифровизации мы ожидаем динамичного роста этого сегмента. Российские компании, ориентированные на внешний рынок, уже давно страхуют эти риски, но массово они все еще не востребованы клиентами», — подчеркнул он.

ПЕРСПЕКТИВЫ ОТРАСЛИ

Общий объем страховых премий на российском рынке по направлению «Киберстрахование» может варьироваться в среднем на уровне 250–300 млн руб. в год, поделился цифрами вице-президент, директор департамента развития небанковских сервисов ПСБ Алексей Назаров. Для сравнения: в 2021-м общий объем страхового рынка в России составил около 1,8 трлн руб., по данным Центробанка РФ. Однако если применение данного инструмента станет обязательным для системно значимых организаций, то, по оценке ряда аналитиков, целевой объем премии в сегменте «Киберстрахование» может достичь примерно 10 млрд руб. в год, добавляет Алексей Назаров.

Пока доля премий в этом сегменте оценивается менее чем в 1% всех видов корпоративного страхования, говорит руководитель управления страхования финансовых рисков «АльфаСтрахования» Алина Малышева.

При этом средняя премия за полис от кибератак в 2021 году составила порядка 50 тыс. руб., приводит данные директор по рискам «СберСтрахования» Владимир Новиков, ссылаясь на Всероссийский союз страховщиков (ВСС). Это свидетельствует о превалировании относительно недорогих решений, содержащих стандартный набор угроз.

Первые общедоступные предложения появились в России в 2017 году, после того как от программ-вымогателей Wannacry и Petya пострадали более 13 тыс. компьютеров. Уже в 2020-м эксперты зафиксировали пятикратное увеличение спроса на услугу, писали СМИ со ссылкой на ВСС. В 2021 году тенденция сохранилась и спрос вырос еще на 60%, приводят результаты исследования аналитики компании «АльфаСтрахование».

ЗАИНТЕРЕСОВАННОСТЬ БИЗНЕСА

Согласно исследованию «РТК-Солар», четверть российских компаний готова тратить средства на страхование киберрисков — 6% респондентов уже пользуются такой услугой, а 21% планируют воспользоваться опцией в будущем. Опрошенные отмечают, что киберстраховка сделает компанию более привлекательной для инвесторов и поможет быстрее восстановиться после инцидента.

«Конечно, отсутствие бюджета — один из ключевых барьеров для приобретения услуги, об этом заявили 33% опрошенных. Но в текущих условиях подобный продукт, напротив, поможет сократить расходы. Восстановление после атак требует расходов, иногда значительных», — говорит Дарья Кошкина.

В основном киберстрахованием интересуются компании с высокой степенью автоматизации бизнес-процессов — торговых, производственных, логистических, отмечает Алина Малышева. Их привлекает в первую очередь страхование убытков в результате простоя бизнеса из-за киберинцидентов. Еще одна актуальная ситуация, по наблюдению эксперта, — это покрытие расходов в результате действия вирусов-шифровальщиков.

Ранее защитой от киберрисков чаще всего интересовались крупные предприятия, но в последнее время внимание проявляют и компании малого и среднего бизнеса, говорит Евгений Ильченко. По его словам, обычно полис приобретают организации, работа которых связана с обработкой и хранением данных. Лидерами в этом виде страхования являются финансовые институты. «У части компаний есть отдельные полисы по киберрискам. Но при этом большинство организаций предоставляют покрытие таких инцидентов как опцию внутри корпоративного страхования», — рассказал эксперт.

Если говорить о банковских каналах продаж, то продукт чаще предлагается именно сегменту малого и среднего бизнеса, поскольку стоимость услуги для компаний с небольшим оборотом сравнительно ниже, чем для крупного бизнеса, указывает Алексей Назаров. Для крупного же бизнеса сдерживающим фактором является ограниченная возможность страховых компаний по принятию больших денежных рисков.

УСЛОВИЯ КИБЕРСТРАХОВАНИЯ

Все страховые компании предлагают разные опции. Тем не менее наличие базовых средств защиты в организации необходимо — в противном случае полис либо не оформят, либо его цена будет очень высокой. Важно соблюдать, что называется, Security Insurance Balance, который подразумевает разумные вложения и в защиту, и в страхование, считает Дарья Кошкина: «Очевидно, что полис не защитит от кибератаки. Поэтому, прежде чем идти в страховую организацию, нужно довести до ума свою ИБ-защиту».

Как правило, полис покрывает риски, связанные с обработкой и хранением данных, например утечки или хакерские атаки. Также он включа-

«ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ» (18+)

Тематическое приложение к «Ежедневной деловой газете РБК»

Является неотъемлемой частью «Ежедневной деловой газеты РБК» № 133 (3626) от 27 октября 2022 г.

Распространяется в составе газеты

Материалы подготовлены редакцией партнерских проектов РБК+

Рекламно-информационный проект: ПАО «МегаФон»

Главный редактор партнерских проектов РБК+: Наталья Кулакова

Редактор РБК+ «Информационные технологии»: Юлия Хомченко-Глуховская

Выпускающие редакторы: Алина Петракова, Марина Зубакова

Дизайнеры: Дмитрий Иванов, Сергей Пивоваров

Фоторедактор: Алена Кондюрина

Корректоры: Татьяна Поленова, Маргарита Тарасенко

Директор по продажам РБК+: Евгения Карлина

ет компенсацию на восстановление деловой репутации, ухудшившейся в результате инцидента, и помощь сотрудникам или клиентам, пострадавшим из-за потери данных. Существуют программы, где утечки и другие инциденты по вине персонала (но не руководства) также входят в страховую защиту, уточняют эксперты.

А вот убытки из-за прекращения подачи электроэнергии или отключения интернета, при том что в собственных системах никаких инцидентов или нештатного функционирования не отмечалось, будут покрыты с ограничениями либо исключены совсем, привела пример Алина Малышева.

Договоры страхования киберрисков чаще всего представляют собой конструктор, где клиент может собрать из блоков подходящую для себя защиту. В «СберСтраховании» также отмечают тенденцию на подбор наполнения полисов под специфические нужды покупателя. Например, активно пользуется спросом покрытие только на случай Dos/DDos-атак.

РЕГУЛИРОВАНИЕ РЫНКА

Пока процедура киберстрахования налажена не до конца, считает исполнительный директор «Смарт-Софт» Сергей Черномашенцев. По его словам, договоры составляются без четких стандартов, а процессы их согласования и проверки идут суперсложно. «Если появится орган, который сможет все это контролировать и регламентировать, то станет намного проще и понятнее. Когда страхование киберрисков будет организовано по принципу ОСАГО или каско, это будет означать, что рынок сформировался и все встало на свои места. Пока процесс хаотичен», — констатирует специалист.

По мнению Евгения Ильченко, для успешного развития рынка необходимо единое законодательное определение киберрисков и четкое понимание последствий для компаний при работе с персональными данными. Эксперт отмечает, что дополнительно важно работать над улучшением безопасности данных в бизнесе, как минимум использовать лицензионное ПО, дублирующие системы и обеспечить корректное хранение данных клиентов и сотрудников.

Александр Гостев в целом обращает внимание на положительную тенденцию в сфере защиты: «Мы видим, что компании больше не экономят на информационной безопасности, тренд, скорее, идет в сторону обеспечения комплексной защиты бизнеса. Все больше компаний применяют экосистемный подход, когда в рамках одной лицензии можно получить уже готовый набор инструментов для полноценной защиты всех элементов инфраструктуры».

25%
российских компаний готовы тратить средства на страхование киберрисков

«Отечественные решения готовы к запросам российского бизнеса»

Директор по развитию корпоративного бизнеса **«МЕГАФОНА» НАТАЛЬЯ ТАЛДЫКИНА** — о том, как на фоне оттока иностранных разработчиков бизнес продолжает ускоренное внедрение технологий и какие отечественные цифровые продукты стали наиболее востребованными после ухода западных поставщиков.

Российские компании демонстрируют закономерно высокий интерес к отечественному софту. Для кого-то это глобальный вопрос продолжения работы, для кого-то — стремление сохранить высокие стандарты ее качества. Бизнес ищет замену ушедшим с российского рынка компаниям и альтернативу оставшемуся без техподдержки ПО. Малому бизнесу в силу масштаба и большей гибкости переход на отечественные продукты дается проще: они были не настолько вовлечены в использование зарубежных решений. Для крупных предприятий перевод на российские продукты сложнее: для них замена систем всегда связана с глобальным пересмотром процессов. Не стоит забывать, что никто не планировал такую стремительную перестройку.

На этом фоне продолжается активная миграция бизнеса в облака. По прогнозу аналитиков IDC, к 2025 году расходы на публичные облачные услуги в России покажут среднегодовой темп роста в 20,4% и превысят $3 млрд. По сравнению с прошлым годом спрос на облачные решения вырос в десять раз. Чтобы иметь возможность быстро удовлетворить его и обеспечить бесшовную миграцию данных новых пользователей, «МегаФон» еще весной приступил к масштабированию мощностей своего облачного сервиса для бизнеса и госсектора. В результате объем свободных ресурсов платформы «МегаФон Облако» удалось нарастить в семь раз. Если судить по нашей практике, то именно офисные решения и инструменты для совместной работы из облака сейчас больше всего интересуют клиентов. Далее идут российские ОС и другое инфраструктурное ПО, попадающее в руки конечному заказчику как сервис.

Отечественные разработки таких сервисов, как видеоконференц-связь, виртуальная АТС, голосовые и текстовые роботы, могут смело конкурировать с западными продуктами. На них также произошел мощный рост спроса. Популярность сервисов для организации видео-конференц-связи объясняется тем, что многие компании использовали инструменты Microsoft, Zoom, Polycom, которые после ухода с российского рынка постепенно перестали поддерживаться.

Для бизнеса выгода там, где есть клиенты и клиентские запросы, поэтому ему очень важно обеспечить контактный центр эффективным решением. Как следствие, растет спрос на импортозамещение на рынке программного обеспечения для корпоративной телефонии и организации контакт-центров. В текущей ситуации зарубежные поставщики не могут гарантировать свое присутствие в России и поддержку, чем подвергают опасности качество доступности компаний для клиентов и снижают эффективность коммуникации между сотрудниками.

Крупные компании ищут замену решениям Cisco, Avaya и Genesys. У «МегаФона» есть решение «Омниканальные коммуникации» — российское on-prem-решение с широкими возможностями. Оно синхронизирует историю взаимодействия с клиентом во всех каналах — чатах, мессенджерах, телефонии, интегрируется с голосовыми помощниками и чат-ботами, работает в защищенной среде — локальной сети контакт-центра или по каналу VPN.

Однако бывают и непростые ситуации, под которые готовых решений нет. Но и тут при должной экспертизе находятся варианты. Так, с одной из консалтинговых компаний «МегаФон» реализовал проект перехода с программного обеспечения Cisco на отечественное решение по организации корпоративной телефонии и омниканального обслуживания в контрактном центре. При этом IP-телефония, которая характеризуется тем, что связь осуществляется между компьютерами и сигнал передается по каналу связи в цифровом виде, при отсутствии доступа в интернет резервируется через каналы традиционной аналоговой телефонной связи.

Преимущество российских провайдеров — в локальности разработок. Оплата происходит в рублях, инструкции и поддержка — на русском, эксперты отвечают быстро и понятно. Развитие продукта заточено под наш темп жизни, культуру и особенности. Например, для одного из клиентов мы доработали конвергентные возможности FMC (технологии, которая помогает создать единую сеть офисных и мобильных телефонов с короткой нумерацией — «экспресс-набором») по принципу территориального разделения по российским почтовым индексам. Неизвестно, сколько бы он ждал этой технологии от ушедшего с рынка крупного западного вендора.

В кибербезопасности самое актуальное направление для миграции с зарубежных вендоров — организация периметра компаний. К ней относится, например, установка межсетевых экранов и систем обнаружения вторжений. Компании ищут новые продукты для защиты периметра и построения надежных каналов связи. Чаще всего клиенты хотят заменить на российские аналоги FortiNet и Cisco. Причем запросы приходят не только на программное обеспечение, но и на программно-аппаратные комплексы, которые устанавливаются в ЦОД и включаются в состав инфраструктуры клиента, которую он арендует у «МегаФона».

Большим спросом также пользуются инструменты защиты от атак на web-приложения и от DDoS-атак, продолжают расти продажи в сегменте продуктов от утечек данных, таких как DLP (Data Loss Prevention) и DAM (Database Activity Monitoring). Еще одно направление, которое, на наш взгляд, останется популярным, — это подключение компаний к центрам мониторинга безопасности. Наше комплексное решение SOC (Security Operations Center) обеспечивает проактивную защиту от всех типов современных киберрисков и может быть развернуто как на инфраструктуре заказчика, так и по облачной модели.

По нашим прогнозам, в 2023 году наиболее перспективными с точки зрения спроса и потенциальной выручки станут платформы виртуализации, аналитические решения для работы с большими данными, операционные системы.

> Преимущество российских провайдеров — в локальности разработок. Оплата происходит в рублях, инструкции и поддержка — на русском, эксперты отвечают быстро и понятно. Развитие продукта заточено под наш темп жизни, культуру и особенности»

Фото: пресс-служба