intelligent enterprise

Владимир Кремер:

«Они не пройдут?»

Помимо самых разнообразных ИТ-систем, нацеленных на решение тех или иных проблем информационной безопасности, можно говорить также о страховании кибер-рисков, обсуждение которого в последнее время перешло в практическую плоскость. Здесь мы преследуем те же цели, что и при внедрении ИБ-продуктов, – снижение рисков информационной безопасности и минимизация последствий инцидентов уже произошедших.

О том, что такое страхование кибер-рисков, как эта деятельность связана с классической активностью компаний в борьбе с угрозами подобного рода, мы беседуем с Владимиром Кремером, руководителем отдела страхования финансовых рисков страховой компании AIG в России.

Intelligent Enterprise: С какими видами киберугроз чаще всего сталкиваются организации? Какие компании страдают от атак в наибольшей степени?

Владимир Кремер: Проблема номер один – целевые атаки на банки, результатом которых становятся существенные убытки, нередко в на миллионы долларов. Не меньшей проблемой являются атаки на системы ДБО [дистанционное банковское обслуживание] как физических, так и юридических лиц. Одной из наиболее актуальных задач, стоящих перед финансовыми институтами, является защита онлайн-порталов и систем интернет-банкинга от мошенничества и хищений. Ключевым вопросом становится поиск решений, позволяющих предотвратить хищение на ранних этапах его подготовки. В связи с отказом от магнитных полос в пользу чипов, которые нельзя взломать, растет количество атак на банкоматы. Широко распространены заражения мобильных телефонов и смартфонов на платформе Android с целью хищения через службы мобильного банкинга.

Все чаще от кибератак страдают средние и крупные корпорации, но сказать, что малый бизнес совсем не подвержен таким атакам, тоже нельзя. Растет и квалификация киберпреступников: подтвержден ущерб в сотни миллионов долларов, причиненный банковской системе России всего одной преступной организацией.

Intelligent Enterprise: Какие меры необходимо принимать для защиты финансовых и других учреждений от киберугроз?

Владимир Кремер: Крайне важно правильно оценить риски и помнить, что при любом киберинциденте компания страдает не только от кражи информации и денежных средств, но и из-за других потерь, особенно репутационных. Среди российских финансовых компаний встречаются самые разнообразные подходы к обеспечению кибербезопасности – от чрезмерной защиты, усложняющей исполнение даже элементарных, выполняемых в ежедневном режиме операций, до легкомысленной уверенности, что их система никогда не станет жертвой преступников.

До разработки систем защиты крайне важно провести исследования двух типов: бизнес-исследование, показывающее, какие процессы приоритетны и должны быть максимально защищены, и обследование ИТ-систем с целью локализации наиболее важных для компании данных и выбора необходимых инструментов защиты. Только после этого можно проводить верхнеуровневую аналитику: какие злоумышленники будут заинтересованы в получении данных и какие сценарии мошенничества могут быть применимы к конкретной компании.

Кроме технических средств защиты компаниям, работающим в финансовой сфере, следует помнить о страховании: оно способствует значительному снижению рисков финансовых потерь, выражающихся в расходах на восстановление данных и расследование, в упущенной выгоде, в перерывах в деятельности, а также потерь (в том числе репутационных), связанных с ответственностью перед клиентами за их данные, которые находятся у компании на хранении и в обработке. Специализированные страховые продукты покрывают расходы не только на услуги сторонних ИТ-специалистов (восстановление поврежденных данных, аудит, оперативное реагирование и расследование киберинцидентов), но и юридические, а также затраты на восстановление репутации.

Intelligent Enterprise: Страхуя, скажем, домашнее имущество, страховая компания по умолчанию уверена, что его владелец предпринимает максимум доступных мер для его защиты. В случае страхования кибер-рисков, очевидно, тоже должна быть уверенность, что в застрахованной компании внедрены определенные ИТ-решения класса ИБ, что заказчик понимает, какие угрозы перед ним стоят, и владеет информацией об их реальном распространении. Все эти вещи как-то учитываются при страховании?

Несомненно, мы проводим беседу с клиентом, планируя заключение страхового договора, если необходимо, привлекаем ИТ-экспертов и специалистов по оценке рисков, обусловленных наличием электронных данных. При этом рассматриваются любые потенциальные инциденты, связанные с информационными технологиями и утечкой данных, и анализируется весь круг последствий для бизнеса – разнообразные убытки как самого бизнеса, так и всех клиентов компании. Установленные у будущего клиента системы информационной безопасности также подвергаются оценке. К сожалению, следует отметить, что даже самые современные системы этого класса не лишены уязвимостей, а у абсолютного большинства компаний нет плана реагирования на киберинцидент. Полученные по результатам подобной оценки данные и заключение эксперта, конечно, влияют на стоимость полиса, и страховые условия – это стандартная ситуация для любого типа страхования.

Intelligent Enterprise: Если зрелость заказчика вами оценена, как вы можете использовать эту информацию на этапе, когда договор страхования кибер-рисков уже заключен?

Владимир Кремер: В связи с растущим количеством киберпреступников и совершенствованием их инструментария растет спрос на услуги экспертов по средствам защиты, предотвращению, анализу и расследованию преступлений в информационной сфере. Помощь таких специалистов включена в наш полис страхования кибер-рисков CyberEdge: мы работаем с лидерами этих направлений – такими компаниями, как K2 Intelligence, Group IB, RSA, Axio Global. Они обладают обширной экспертизой в области ИТ, следят за техническими новинками и возможностями информационной сферы, успешно применяя их на практике в течение многих лет, предоставляют услуги по аналитике и консалтингу, защите информации и расследованиям инцидентов.

Поэтому доступ к их сервисам – ключевое преимущество современного и актуального страхового продукта.

Intelligent Enterprise: Сегодня часто говорят о вполне определенных технологиях автоматизации бизнеса, таких как большие данные, Интернет вещей, облачные или мобильные вычисления. Влияет ли их распространение на структуру приоритетов конкретных кибер-рисков и на потребности в страховании?

Владимир Кремер: Конечно, влияет, и поскольку увеличивается количество данных, растёт трафик, усложняются системы – однозначно растут и риски. Любой страховой продукт должен чутко реагировать на все изменения в той сфере, которую он защищает, поэтому структура полисов постоянно изменяется. Мы внимательно следим за состоянием киберпреступности и анализируем тенденции. Так, в 2014 году главным каналом утечек конфиденциальной информации в мире стали браузеры и облачные хранилища. Отсюда следует, что именно компании, активно использующие облака, сегодня находятся в зоне повышенного риска и постепенно осознают пользу страхового полиса, покрывающего инциденты утечек из хранилищ такого типа.

Intelligent Enterprise: Сегодня продуктовая ИТ-стратегия некоторых российских компаний меняется. Тенденция импортозамещения в сфере прикладных ИТ-систем или переориентация на иные зарубежные рынки может так или иначе повлиять и на структуру кибер-рисков. Это как-то учитывается вашей компанией?

Владимир Кремер: Основной кибер-риск – хакерство и вредоносные коды – является внешним и в высокой степени международным, поэтому не зависит от стратегии импортозамещения. Не имеет большого значения, где

произведены комплектующие ваших ИТ-устройств: если они подключены к Интернету, ваши риски сразу становятся глобальными. Тем не менее некоторых перемен, связанных с ужесточением требований со стороны государственных органов, которые устанавливают всё более жёсткие стандарты для компаний, работающих в России и с российскими данными, очевидно, следует ожидать.

Intelligent Enterprise: В настоящее время осведомленность отечественных компаний в отношении различных ИТ-систем информационной безопасности уже нельзя признать низкой, хотя практика их применения еще явно недостаточна. Но о страховании кибер-рисков известно еще меньше. Какие мероприятия проводятся для информирования организаций?

Владимир Кремер: Со своей стороны мы стараемся, чтобы профессиональное сообщество как можно больше узнало о наиболее актуальных кибер-рисках и способах их минимизации, и для этого распространяем информационные материалы, выпускаем авторские статьи в деловых изданиях и проводим специализированные мероприятия. Одну из своих задач мы видим в повышении осведомленности о таких рисках среди российского профессионального сообщества и всегда готовы поделиться своей международной экспертизой.

Помимо этого мы регулярно проводим конференции и бизнес-встречи на тему кибербезопасности и принимаем активное участие в мероприятиях наших партнеров по данной тематике: с начала 2015 года состоялись четыре подобные встречи. В рамках данных мероприятий были представлены доклады экспертов из сферы расследования киберпреступлений и страхования кибер-рисков, ИТ-специалистов, представителей крупнейших финансовых организаций страны.

Но основным фактором, повышающим уровень защищённости наших клиентов, мы считаем присутствие в нашем страховом продукте CyberEdge, над улучшением наполнения которого мы постоянно работаем, а также раздела по предотвращению страховых случаев. Этот раздел обеспечивает доступ наших клиентов к услугам специалистов ведущих мировых компаний в области кибербезопасности, о которых я уже говорил: RiskAnalytics, K2 Intelligence, IBM, BitSight, RSA, Axio Global, Group IB.

Intelligent Enterprise: А требует ли услуга страхования CyberEdge, которая, как известно, предоставляется на международном рынке, локализации в России?

Владимир Кремер: Мы имеем огромный зарубежный опыт в этом страховании и сотрудничаем с глобальными компаниями – специалистами в области кибербезопасности, делая их экспертизу и услуги доступными для наших российских клиентов. В то же время в России наши клиенты могут воспользоваться услугами Group-IB – отечественного лидера сферы кибер-расследований. Для работы с репутационным риском по причине киберинцидента наши российские клиенты могут выбирать между известными международными PR-агентствами и отечественным коммуникационным агентством КРОС. И так – со всеми компаниями и специалистами, услуги которых мы оплачиваем по полису.

В целом все наши клиенты на российском рынке имеют возможность получить не меньший объем ИТ-, юридических и PR-услуг, нежели в других странах. Единственная разница пока – в проникновении этого вида страхования: на данный момент действующих договоров по страхованию кибер-рисков в России сравнительно немного, и можно сказать, что сейчас мы скорее обучаем рынок, показываем потенциальным клиентам, какие риски могуть быть предотвращены при помощи данного вида

страхования. Клиенты проявляют заинтересованность: хотят понять, что дает этот продукт, готовы анализировать правила страхования. Развитие законодательства и нормативной базы в сфере ИТ, а также последние инициативы регуляторов позволяют нам предполагать, что страхование кибер-рисков будет широко востребовано в России в ближайшие пять лет. В настоящий момент очевидный интерес к нашим услугам на отечественном рынке проявляют банки, розничные компании, предприятия телеком-индустрии, а также компании энергетической отрасли.

С Владимиром Кремером беседовал ведущий эксперт Intelligent Enterprise Сергей Костяков