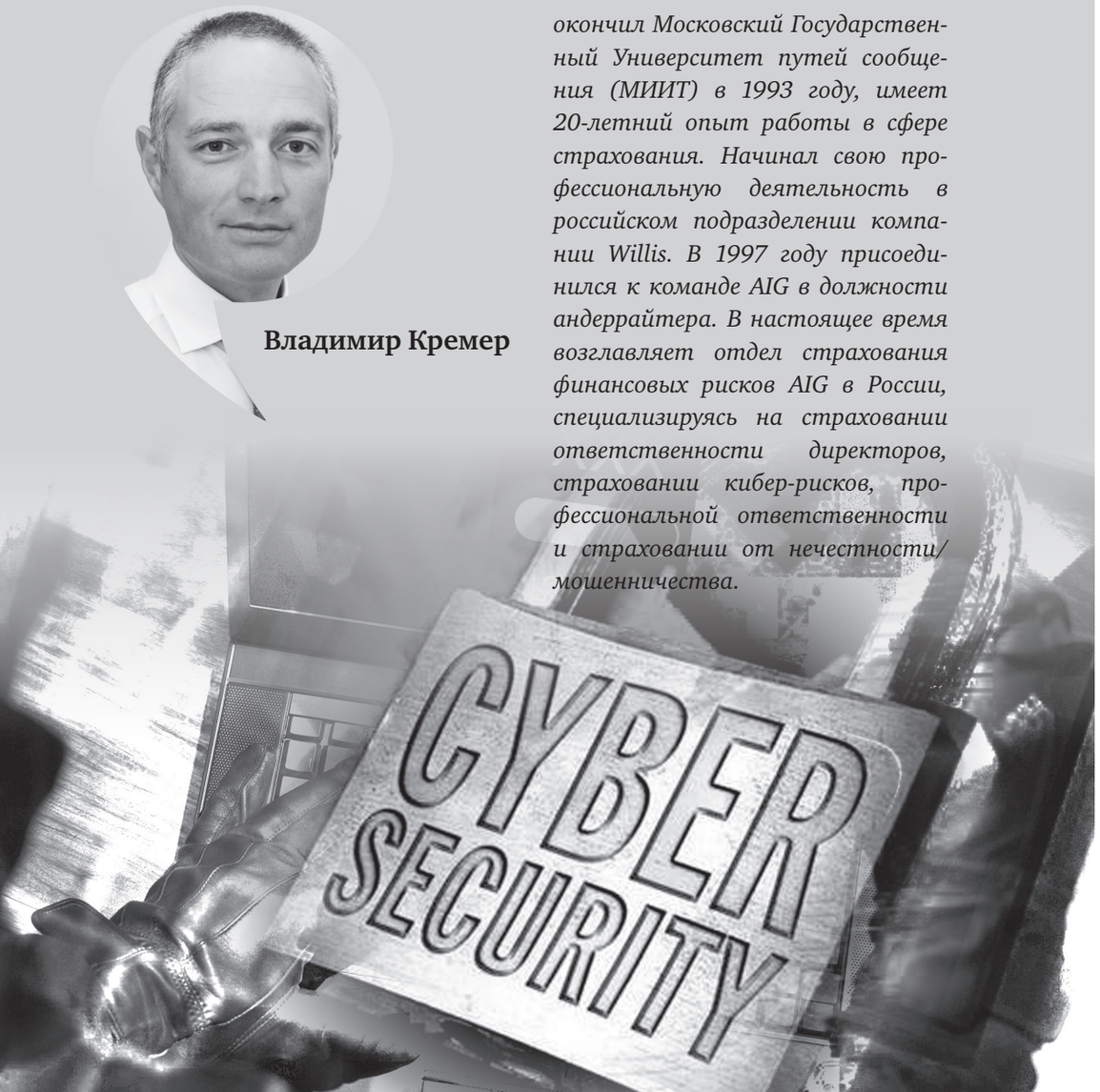
КИБЕР-РИСКИ – ЭТО СЕРЬЕЗНО



Владимир Кремер

окончил Московский Государственный Университет путей сообщения (МИИТ) в 1993 году, имеет 20-летний опыт работы в сфере страхования. Начинал свою профессиональную деятельность в российском подразделении компании Willis. В 1997 году присоединился к команде AIG в должности андеррайтера. В настоящее время возглавляет отдел страхования финансовых рисков AIG в России, специализируясь на страховании ответственности директоров, страховании кибер-рисков, профессиональной ответственности и страховании от нечестности/мошенничества.

Все чаще крупные клиенты при принятии решения о сотрудничестве требуют от своих партнеров наличия полиса страхования кибер-рисков, осознавая, что их данные постоянно находятся под угрозой и нуждаются в защите. И это не случайно, сегодня компании более подвержены угрозам сетевой безопасности и конфиденциальности, чем когда-либо.

Потенциальные клиенты

Сообщения о случаях взлома IT-систем появляются в СМИ регулярно, и все чаще в них фигурируют названия крупнейших компаний, работающих в самых разных сферах, всемирно известных знаменитостей, а иногда даже высокопоставленных политиков. Так, в конце 2014 года в американской прессе широко освещался скандал, связанный со взломом хакерами одного из самых посещаемых сайтов в США www.forbes.com. Пользователи, которые посетили этот сайт с 28 ноября по 1 декабря, были подвержены хакерским атакам. Недавно на короткое время была также взломана лента Twitter Newsweek, в которой злоумышленники успели опубликовать сообщения, направленные против президента США Барака Обамы, первой леди и их дочерей. В декабре 2014 года несколько демо-записей незавершенного альбома поп-звезды Мадонны Rebel Heart были выложены в Интернет, заставив суперзвезду поспешно выпустить шесть треков и перенести дату выхода полноценного альбома, который изначально должен был выйти в марте. Певица поблагодарила израильские правоохранительные органы за оказание помощи по задержанию хакера в Тель-Авиве, который взломал ее компьютерную систему и выложил в Интернет ранее неизданную музыку.

В том же месяце хакерским атакам подвергся гигант киноиндустрии Sony Entertainment Pictures, вследствие инцидента конфиденциальные корпоративные данные компании просочились в Интернет. В результате, по заявлению компании, в текущем квартале они планировали потратить 15 млн долларов на расследование и восстановление после убытков, связанных с вышеупомянутой кибер-атакой. Несмотря на это, факт, что инцидент обойдется Sony в $15 млн, является наглядным примером того, как дорого может стоить кибер-преступление для бизнеса, и почему адекватные меры обеспечения безопасности имеют жизненно важное значение.

Такие атаки происходят каждый день, и мотивы преступников, которые решаются на взлом IT-системы той или иной организации, могут быть самыми разными. Пострадать от хакеров могут предприятия разной сферы деятельности. Ошибочно считать, что средние и мелкие предприятия не подвергаются кибер-атакам только потому, что, если «королевство маловато», то и хакерам «развернуться негде». Ко-

нечно. иногда кибер-преступники используют небольшие компании, как точку доступа к большим, более желанным целям. Но чаще всего небольшие компании становятся «легкими» мишенями, потому что у них нет ресурсов для организации эффективной системы безопасности.

По данным исследования, проведенного Лабораторией Касперского и B2B International в 2014 году, DDoS атаки на интернет-ресурсы компании могут привести к значительным убыткам – в среднем от 52 до 444 тысяч долларов, в зависимости от размера предприятия. Такие непредвиденные расходы для многих организаций являются серьезным обременением. Атаки хакеров также могут нанести вред репутации предприятия из-за длительного отсутствия доступа к его онлайн-ресурсам и вылиться в дополнительные еще более серьезные финансовые потери.

В целом, компании, подвергшиеся кибер-преступлению, можно разделить на три группы. Первые – слишком остро реагируют на случившиеся и делают скоропалительные публичные заявления. Вторые – недооценивают событие и ждут несколько дней (а иногда – недель), чтобы начать действовать. К третьей группе относятся те компании, у которых есть четкий план действий, благодаря которому они могут оперативно разобраться в сложившейся ситуации и минимизировать последствия.

Как правило, пострадавшей от действий хакеров компании требуется пул специалистов, который может быстро отреагировать на случившееся и предпринять меры. Но содержать в штате целую команду высококлассных юристов, IT и PR-менеджеров, которые могут потребоваться в случае взлома IT-системы, не всегда целесообразно, проще купить страховой полис, который в таком случае и обеспечит компании услуги соответствующих профессионалов. Практика показывает, что в периоды нестабильной политической обстановки количество DDoS-атак возрастает. Также особенно актуальными программы страхования кибер-рисков становятся в периоды экономических кризисов.

В России же потенциальный рынок кибер-страхования огромен, поскольку в такой страховой защите нуждаются предприятия самых разных отраслей и категорий.

По данным исследования, проведенного Лабораторией Касперского и B2B International в 2014 году, DDoS атаки на интернет-ресурсы компании могут привести к значительным убыткам – в среднем от 52 до 444 тысяч долларов, в зависимости от размера предприятия.

Производство. Энергетические компании. Промышленность

Производственным и промышленным предприятиям нужны комплексные и надежные системы для обеспечения непрерывности производственного процесса, процессов отгрузки и т.д. Как показывает практика, кибер-угрозам на производственном предприятии подвержены системы снабжения, системы дистрибуции, клиентские базы данных и даже корпоративный интранет и полностью изолированные от «внешнего мира» внутренние информационные системы.

Розница

Предприятия розничной торговли владеют огромным количеством информации о клиенте, включая номера кредитных и дебетовых карт, эта информация может привлечь потенциального преступника и стать поводом для взлома IT-системы розничной сети. Причем клиенты розницы, которые обычно используют одинаковые пароли и сохраняют регистрационные данные в нескольких аккаунтах, в данном случае подвергаются еще более серьезной опасности, так как становятся более уязвимыми к атакам хакеров. Простые, одинаковые пароли, сохраненные данные легко распознаются современными мошенниками.

Сфера услуг, здравоохранение

Существенный объем электронных данных по ведению состояния здоровья больного, данные платежных карт пациентов, базы персональных данных клиентов сделали эти отрасли намного более уязвимыми для сбоев систем безопасности, чем любые другие.

Как правило, пострадавшей от действий хакеров компании требуется пул специалистов, который может быстро отреагировать на случившееся и предпринять меры.

Банки. Финансы

Финансовые институты всегда были подвержены атакам хакеров, а это ставит в опасность конфиденциальные данные. Вредоносные программы, не авторизированные устройства и бизнес-приложения от третьих лиц – все это создает проблемы для банков и других финансовых институтов.

Крупные предприятия

Большинство крупных предприятий считают, что «их IT-департамент эффективно справляется с кибер-рисками», и не воспринимают возможную опасность кибер-атаки всерьез, что влечет за собой реальные проблемы в случае ее возникновения.

Малый и средний бизнес

Малые и средние компании могут владеть большим количеством ценной информации, и при этом использовать устаревшие IT-системы на своих предприятиях, так как их бюджет на обеспечение информационной безопасности и закупку современного ПО и оборудования ограничен.

Полис CyberEdge

Согласно статистике, AIG помогла справиться с кибер-атаками более тысячи компаний и двадцати миллионам человек в разных странах мира, которые в свое время приобрели страховую защиту от кибер-рисков в нашей компании. Для обеспечения информационной защиты персональных данных на предприятии от последствий их утечки или незаконного использования

AIG предлагает для страхователей инновационный пакет CyberEdge, страховое покрытие которого включает:

– *страхование ответственности, связанной с использованием персональных данных или корпоративной информации*, то есть покрытие убытков страхователя, включая расходы на защиту в суде, возникающие в результате требований против него по утверждаемым или фактическим нарушениям в отношении персональных данных или корпоративной информации;

– *страхование от перерыва в деятельности предприятия/сети (дополнительная опция)*: покрытие убытка предприятия в виде потери чистой прибыли в результате длительного перерыва в функционировании информационной сети, вызванного атакой на сетевые ресурсы и сервисы компании с целью приостановления ее деятельности, затруднения доступа к сетевым ресурсам, либо нарушения системы безопасности сети;

– *страхование ответственности за содержание информации (дополнительная опция)*: покрытие убытков и расходов в результате публичного раскрытия информации, вызванного заявленным или фактическим действием, ошибкой, ложным заявлением, вводящим в заблуждение заявлением или упущением в связи с деятельностью в области мультимедиа;

– *страхование от виртуального вымогательства (дополнительная опция)*: покрытие расходов, понесенных, с письменного согласия страховщика, для ограничения или прекращения угрозы безопасности, которая может повлечь за собой убыток для страхователя;

– *страхование от издержек вследствие расследования со стороны регулирующих органов*: покрытие потенциально крупных издержек и расходов, связанных с проведением расследований регулирующими органами;

– *антикризисный PR*: услуги по реагированию в случае утечки данных – восстановление репутации компании или личности, инструктаж на случай утечки персональных данных, а также расходы на уведомления и мониторинг, возникающие в связи с утечкой информации;

– *электронные данные*: покрытие расходов, связанных с восстановлением, повторным сбором или введением информации после утечки или несанкционированного использования данных.

Согласно статистике, AIG помогла более тысячи компаний и более чем двадцати миллионам человек справиться с кибер атаками, которые в свое время приобрели страховую защиту от кибер-рисков в нашей компании.

Практический опыт AIG в урегулировании страховых событий подтверждает, что наша компания обладает уникальными возможностями, которые позволяют не только выявить, но и предвосхитить страховой случай.

Рассмотрим несколько последних страховых случаев в области взлома и доступа к данным клиентов: сервисная компания подверглась взлому, в результате которого были похищены личные данные – информация о клиентах. Данный страхователь ведет деятельность в 70 странах мира и содержит около 286 000 отдельных записей данных. Внешняя компания по обеспечению безопасности уведомила страхователя о взломе его систем. Были задействованы юридические услуги и услуги мониторинга. Следующий взлом произошел пять недель спустя, и был совершен тем же преступником. Стало очевидно, что системы страхователя находились под постоянной атакой после обнаружения первого взлома. Хакер использовал уязвимые места в веб-системах компании и использовал их как точку входа во внутреннюю сеть. В результате взлома хакер смог получить доступ к личным данным. Преступник принадлежал к высококвалифицированной команде хакеров, которая была заинтересована в конкретных данных, и впоследствии была арестована ФБР. На сегодняшний день было предпринято судебное расследование и проведено восстановление систем сервисной компании. Все субъекты данных были уведомлены о взломе. Им был предложен кредитный мониторинг и страхование от кражи персональных данных.

4 830 человек пострадали, когда внутреннее напоминание сотрудникам об истечении срока получения кредита на оздоровительные услуги было случайно отправлено по электронной почте другим сотрудникам.

Страхователь получил консультации в области PR по управлению репутацией. Все данные в настоящее время хранятся на чистых серверах с обновленной и расширенной системой безопасности. Общая сумма выплаты составила 906 тысяч долларов.

Другой страховой случай не повлек за собой иски и финансовые убытки, но заслуживает внимания в связи со своим масштабом и особым, «деликатным» характером раскрытых данных. У страхового брокера были похищены данные о сотрудниках: произошел взлом данных в отношении программы покрытия медицинских расходов по региону деятельности страхователя. 4 830 человек пострадали, когда внутреннее напоминание сотрудникам об истечении срока получения кредита на медицинские услуги было случайно отправлено по электронной почте другим сотрудникам. В тексте напоминания содержалась личная информация о сотрудниках, которые попадают под действие программы. Страхователь провел внутреннее расследование и в настоящее время считает, что информация не была неправильно использована, и все копии случайно раскрытой информации были удалены. Страхователь уведомил о случившемся судебные, надзорные государственные органы. По происшествию не было подано

никаких претензий, отсутствуют угрозы каких-либо судебных исков. Страхователь обладает полисом страхования кибер-рисков – в настоящее время дело рассматривается в соответствии с основным полисом.

Еще один случай затронул более одного миллиона клиентов сети оператора интернет-игр, которая пострадала от сбоя. Было подано семь коллективных судебных исков, связанных со сбоем. Используя ресурсы своей обширной сети партнеров, AIG работала в тесном сотрудничестве со страхователем, чтобы привлечь юридическую компанию для защиты в суде, экспертную IT-компанию для расследования нарушения, компанию, специализирующуюся на оказании маркетинговых услуг в области цифровых каналов коммуникаций и компанию по связям с общественностью для борьбы с негативной реакцией средств массовой информации. AIG урегулировала судебный иск за 1,5 млн. долларов, не подвергая своего страхователя длительному и дорогостоящему процессу судебного расследования

И в заключении стоит упомянуть страховой случай в специализированной сети торговли автозапчастями. ИТ-менеджер компании обнаружил, что файл, который не был частью сайта компании, использовался для кражи информации о платежных картах. От имени страхователя – платежной системы, AIG помогла продавцу привлечь эксперта-аудитора и возместила 7 тысяч долларов за экспертную проверку и 3,5 тысячи долларов сборов и штрафов компании-эмитенту кредитных карт.

Важно отметить, что в практике AIG встречались совершенно разные по специфике и размерам ущерба случаи – иногда инциденты, вызывающие незначительные или и вовсе отсутствующие материальные убытки, могут стать причиной существенного ущерба репутации страхователя (так, один из вышеописанных случаев мог привести к серьезному ущербу бренда работодателя). Зачастую, столкнувшись с кибер-атакой, компании не могут оперативно скоординировать работу своих юридических, IT и маркетинговых отделов, чтобы должным образом отреагировать на критическую ситуацию. Тогда включение в полис услуг экспертов во всех этих областях, таких как специалисты по маркетингу в диджитал-сфере в третьем описанном кейсе, может стать настоящим спасением. Опыт AIG и ее многочисленных клиентов по всему миру демонстрирует, что полис страхования кибер-рисков оказывается одинаково полезен во всех ситуациях вне зависимости от масштаба атаки и нанесенного ущерба.

Зачастую, столкнувшись с кибер-атакой, компании не могут оперативно скоординировать работу своих юридических, IT и маркетинговых отделов, чтобы должным образом отреагировать на критическую ситуацию.

ЗАЩИТА ПО-МОСКОВСКИ

Николай Рубцов

профессиональный строитель, имеет опыт работы в Госстрое РФ, в СК «МАКС» трудится с 1994года. Единственный представитель страховых компаний, кто участвовал в составе рабочей группы, создавшей «Программу льготного страхования жилья» в Москве. В настоящее время является заместителем генерального директора СК «МАКС»