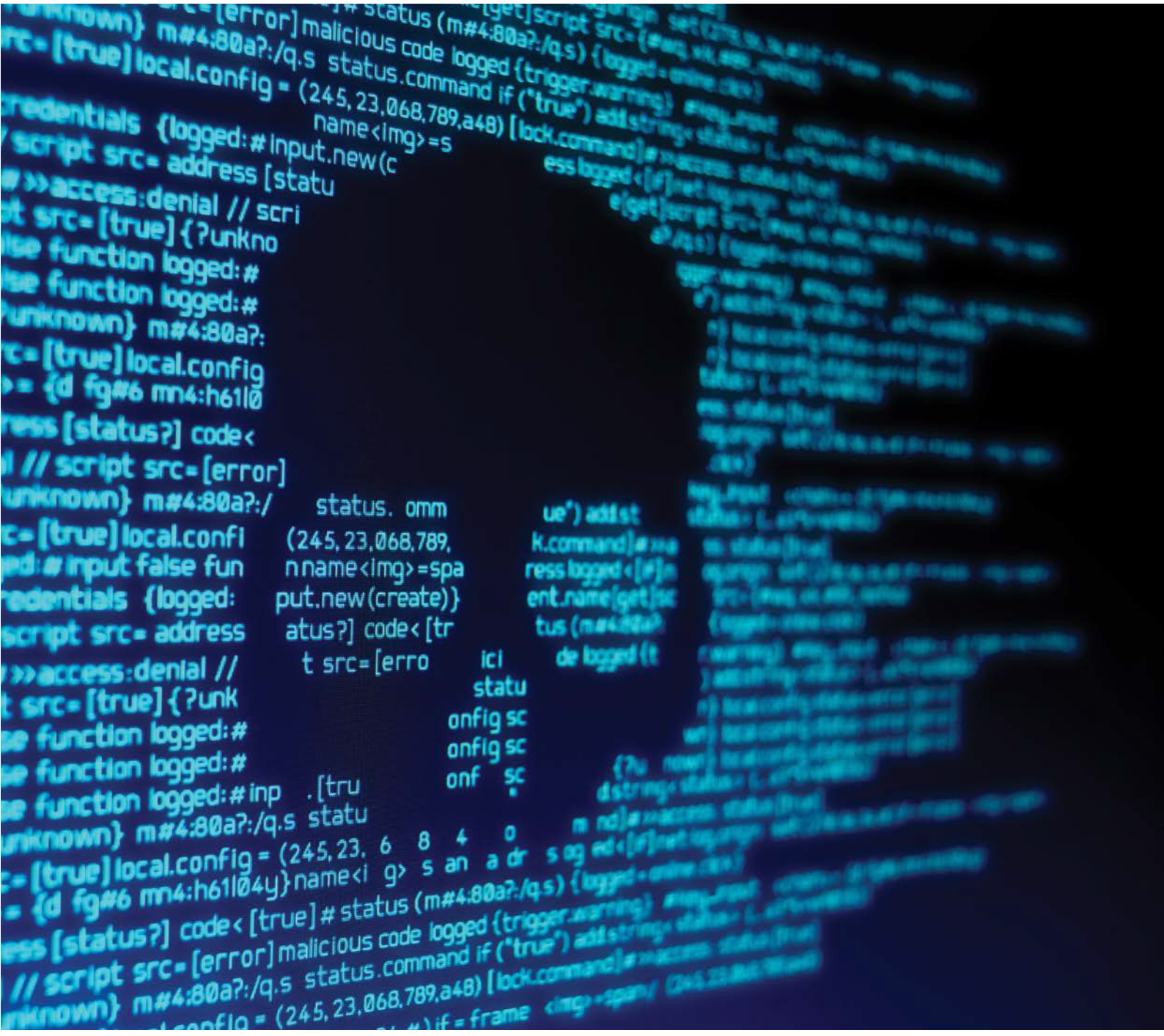
Серия аналитических материалов
по урегулированию страховых случаев



Страхование киберрисков: программы-вымогатели – реальная угроза для бизнеса

Статистика убытков по страхованию киберрисков в AIG за последние годы отражает не только рост количества страховых случаев по договорам страхования, но и дает представление об угрозах, которые в последние месяцы характеризовались серией сложных системных атак с использованием вредоносных программ и программ-вымогателей, включая WannaCry и Petya. Самые серьезные последствия для европейских компаний имели такие убытки как перерыв в производстве и недоступность сети, однако большинство таких убытков оказались незастрахованными.

2017-2018 годы характеризуются массовыми атаками с использованием программ-вымогателей, в результате которых компании нередко были вынуждены приостановить свою производственную деятельность. Статистика страховых случаев AIG показывает, что программы-вымогатели были основной причиной убытков, связанных с киберрисками в 2018 году (26%, что составляет более четверти страховых случаев). Это существенный рост против показателя 16% в 2014-2018.

«Похищение инструментов Агентства национальной безопасности США, с одной стороны, и возможности государств спонсировать атаки – с другой, в сочетании привели к катастрофическим событиям», – говорит Марк Камилло, руководитель направления киберрисков AIG в регионе EMEA. «Последствия Wannacry, поразившего сотни тысяч компьютеров по всему миру, могли бы быть намного серьезнее с точки зрения масштабов и застрахованных убытков, если бы британский эксперт оперативно не нашел и активировал экстренное аварийное отключение».

Следом за программами-вымогателями и взломом данных, основными типами атак можно назвать нарушения работы системы безопасности, несанкционированный доступ и мошенничество при помощи имперсонации. Доля убытков, вызванных с небрежностью сотрудников, незначительно снизилась до 7% в 2018 году, при этом человеческий фактор остается одной из основных причин большинства киберпроисшествий.

Основные выводы

- В 2018 году количество полученных AIG заявлений о страховых случаях было равным количеству заявлений, полученных за предыдущие четыре года вместе взятых, по одной претензии за рабочий день.
- Программы-вымогатели остаются главной причиной киберубытков (при этом перерыв в производстве является основным их последствием). Наблюдается увеличение количества атак по всему миру.
- Отрасли розничной торговли, профессиональных и финансовых услуг находятся в первых строках списка, когда речь идет о киберубытках. Инциденты происходят в широком спектре секторов, а это значит, что ни одна отрасль не защищена от кибератак.

Рис. 1 **Киберубытки, заявленные клиентами AIG EMEA в 2018 г.**

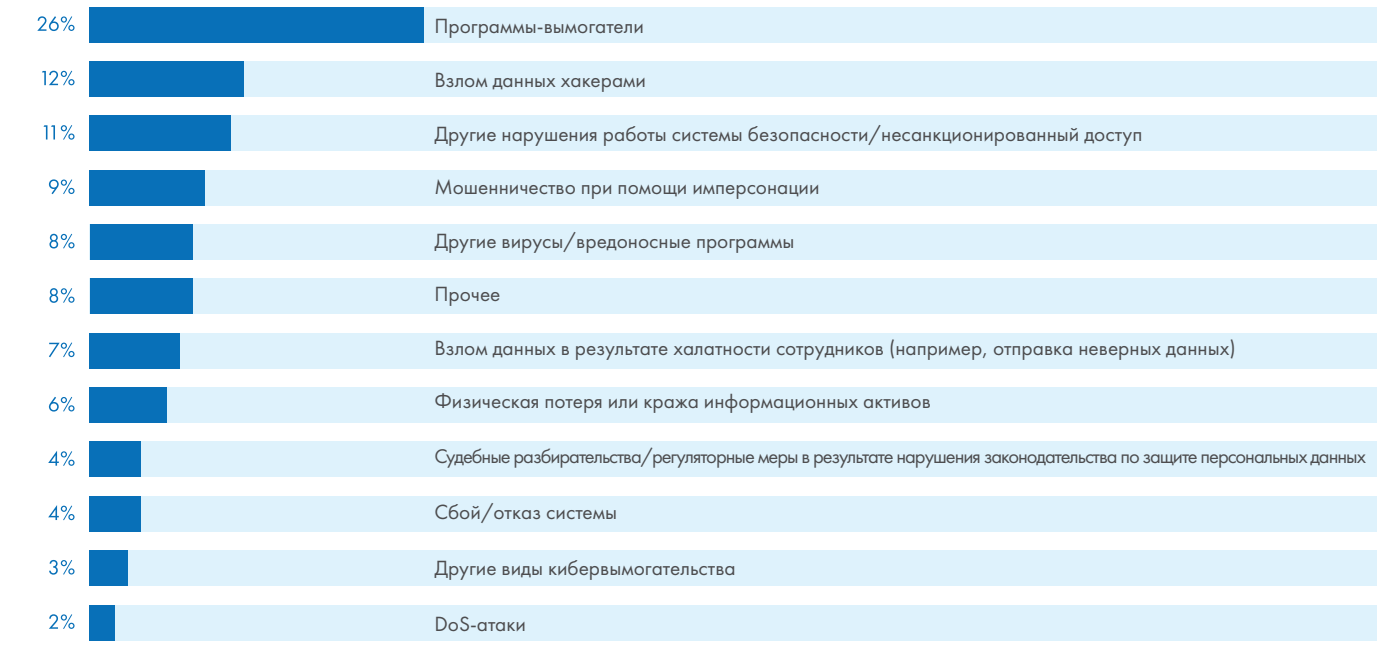
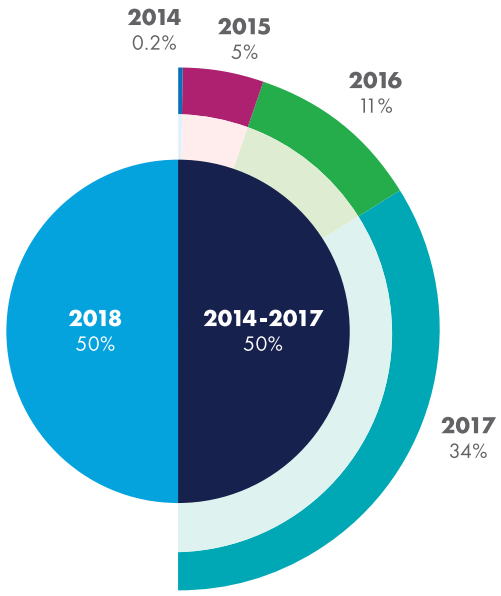


Рис. 2 **Динамика киберубытков, заявленных клиентами AIG EMEA , 2014-2018**

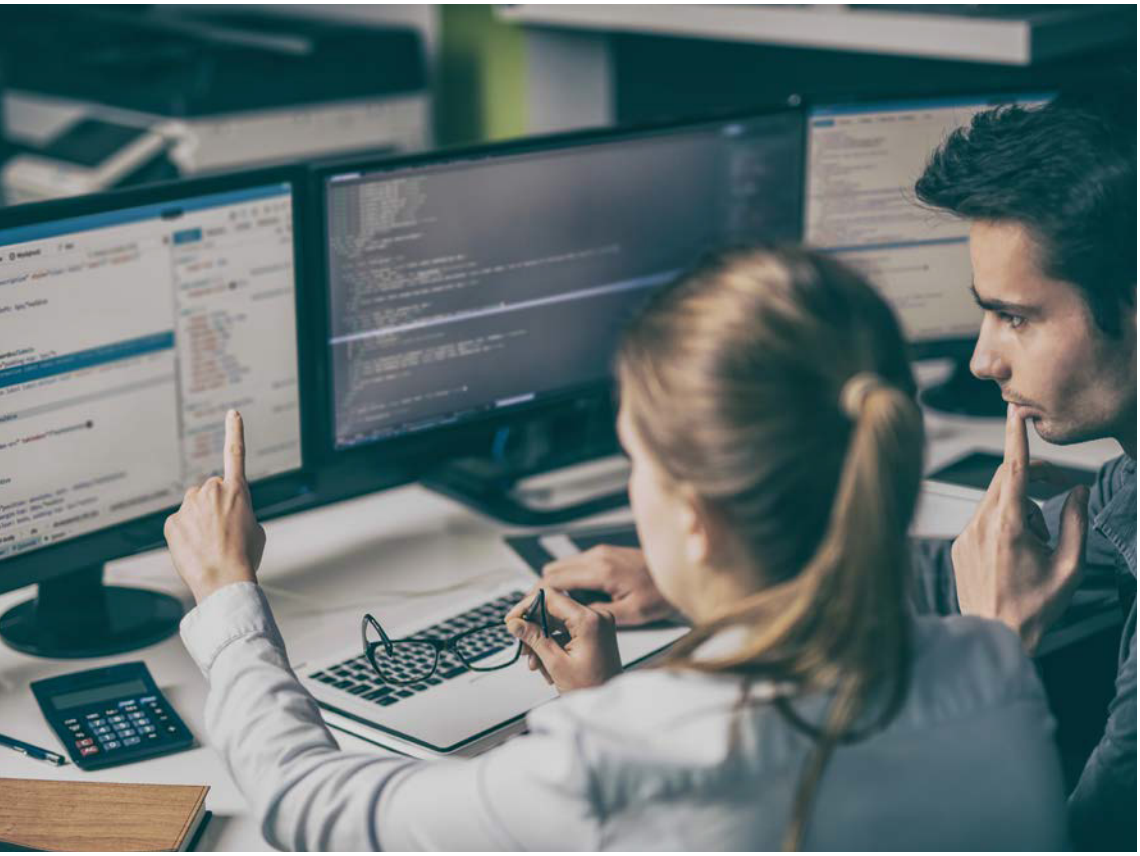


В 2018 году также увеличилась частота убытков, когда специалисты AIG по урегулированию киберрисков каждый день фиксировали получение как минимум одно заявление о получении возмещения. Рост частоты убытков отражает тенденцию к увеличению масштабов кибератак.

Приобретение страхового покрытия от киберрисков становится более распространенным среди множества организаций, поэтому у покупателей появилась возможность ближе познакомиться с содержанием продукта. Теперь они лучше понимают объем покрытия, какие события покрываются полисом страхования, что можно и нужно заявлять страховщику.

Внимание к теме страхования киберрисков значительно выросло после волны системных DDoS-атак и случаев использования программ-вымогателей. Это само по себе будет способствовать увеличению частоты убытков в будущем. «Сейчас мы наблюдаем всплеск интереса со стороны нетипичных покупателей киберстрахования, поэтому мы прогнозируем увеличение количества убытков по сравнению с прошлым годом только исходя из показателей роста страховых премий», – отмечает Марк Камилло.

«Последствия Wannacry, поразившего сотни тысяч компьютеров по всему миру, могли быть намного серьезнее с точки зрения масштабов и застрахованных убытков...»
Марк Камилло



Угроза для всех отраслей

Статистика убытков AIG подтверждает, что ни один сектор не защищен от кибератак. В 2018 году киберубытки были заявлены страхователями из восьми отраслей, которые ранее вообще не фигурировали в статистике киберубытков AIG. Это постоянный тренд: каждый год все больше заявлений об убытках поступает от широкого круга отраслей промышленности, например, энергетика и транспорт, а не только традиционно связанных с киберрисками отраслей.

Страховые случаи по-прежнему затрагивают отрасль финансовых услуг, но доля этого сектора в 2018 году снизилась (до 18%, по сравнению с 23% в 2014-2017). Сама природа банковского и страхового бизнеса и то, что финансовые учреждения собирают и хранят огромные объемы персональных данных и подвергаются строжайшему регулированию (а также возможным крупным штрафам), означает, что компаниям сектора финансовых услуг всегда нужен надежный подход к киберрискам.

Рис. 3 **Киберубытки, заявленные клиентами AIG EMEA в 2018 г. по отраслям**

* Продукты питания и напитки, строительство, недвижимость, сельское хозяйство, информационные услуги.

Примечание: в сумме цифры могут не составлять 100% из-за округления

Однако сокращение доли убытков финансовых учреждений может лишь отражать устойчивый рост претензий со стороны других отраслей в связи с увеличением объема заключенных договоров страхования AIG в регионе EMEA. По словам Марка Камилло, «сегмент финансовых услуг для нас всегда был одним из самых больших, но с прошлого года мы наблюдаем, как покрытие начали покупать компании из других отраслей».

«Многие из последних атак с использованием программ-вымогателей были неизбирательными с точки зрения отрасли, на которую они нацелены», – продолжает эксперт. «Если у пользователей определенного программного обеспечения есть уязвимость, именно на них будут направлены ковровые бомбардировки, подобные тем, что мы наблюдали в 2018. Интересно, будет ли больше целенаправленных атак в 2019 году, особенно с нынешней политической ситуацией, созревшей для деятельности, финансируемой государствами».

В общем объеме убытков значительно выросла доля отрасли профессиональных услуг (с 6% до 18% за 2014-2017 гг.), в то время как доля других секторов, исторически больше связанных с киберрисками, уменьшилась. «Отрасль профессиональных услуг становится более частой мишенью для кражи данных», – утверждает Кэти Эйвери, специалист AIG по урегулированию крупных финансовых убытков. «Конечно юристы и бухгалтеры с большими клиентскими базами данных привлекательны для киберпреступников из-за качества информации, которую они хранят, и уязвимы для киберпреступлений, нацеленных на регулярные финансовые транзакции».

«По-прежнему находятся руководители компаний, которые думают «это не произойдет со мной и моим бизнесом» или «у меня нет никаких важных данных, почему же я могу стать их мишенью?» Но даже если компания не хранит важные данные, она все равно может стать жертвой программ-вымогателей. А если в результате атаки файлы будут зашифрованы, бизнес не сможет функционировать», – добавляет она.

«Компании отрасли профессиональных услуг, в том числе юридические и бухгалтерские фирмы, становятся более частой мишенью для кражи данных». Кэти Эйвери

Программы-вымогатели становятся товаром массового потребления

От масштабных системных атак пострадали компании большинства европейских стран. WannaCry был нацелен на уязвимость Windows, которая использовалась для распространения вредоносного ПО на сотни тысяч компьютеров в более чем 150 странах. Под ударом оказались компании из многих отраслей, включая здравоохранение, финансовые услуги, логистику, образование и промышленное производство.

За последние 24 месяца программы-вымогатели стали переходить в товарную форму, а создатели новых версий предлагают соглашения о разделении доходов с «партнерами-аффилиатами». Больше нет гарантий, что страхователь получит обратно свои данные, даже если заплатит выкуп. «Профессиональный подход» на ранних стадиях вымогательства, когда колл-центры общались с жертвами для получения биткойнов в качестве оплаты выкупа и восстановления данных, теперь почти ушли в прошлое.

Однако «программы-вымогатели как услуга» по-прежнему представляют угрозу. Компания может думать, что ее данные не важны или не подвержены рискам, но опыт урегулирования страховых случаев в 2018 году показал, что атаки с помощью программ-вымогателей в значительной степени неизбирательные, и могут быть направлены на организации любых отраслей и размеров. AIG прогнозирует, что автоматизация и коммодитизация программ-вымогателей продолжится, а физические и юридические лица столкнутся с еще большим количеством атак.

Также есть ожидания смещения акцента в сторону «криптоджекинга»[1]. Только за 2017 год крипторынок вырос более чем на 1200%[2]. Увеличение стоимости электронных валют привлекает внимание киберпреступников, которые все чаще используют вредоносное ПО для майнинга.

В будущем ожидается, что в традиционных формах вымогательства будет применяться целевой взлом данных. Сейчас эта тенденция больше актуальна для американского рынка, хотя европейские компании, преимущественно те, которые представлены в США, также страдают от взлома данных. Новый общий регламент по защите данных в Европе (GDPR), вероятно, станет еще одним инструментом для вымогателей, которые будут угрожать компрометацией данных организации в случае отказа заплатить выкуп, зная, что в соответствии с новым правовым режимом последствия будут более тяжелыми.

Масштабные убытки в результате недоступности сети

Статистика убытков показывает, что доля сбоев в работе бизнеса в качестве основного источника убытков (так называемая «недоступность сети» при констатации перерыва в производстве из-за киберрисков), снизилась по сравнению с аналогичным периодом 2014-2017 гг. При этом перерыв в производстве в 2018 году стал существенной проблемой для многих европейских организаций. Убытки в результате недоступности сети стали причиной многих страховых случаев, но они не всегда определялись как основная причина, поэтому такие убытки недопредставлены в статистике претензий.

«Довольно часто в момент заявления о событии страхователи не понимают, в чем именно заключается их убыток», – объясняет Мартин Овертон, специалист по киберрискам AIG в регионе EMEA. «Они считают, что это просто вирус или попытка вымогательства. И только после привлечения команды экспертов и глубокого погружения в проблему, клиент осознает, что инцидент повлияет на его бизнес, так как он не может получить доступ к данным или его системы выведены из строя».

[1] https://www.forbes.com/sites/jasonbloomberg/2018/03/04/top-cyberthreat-of-2018-illicit-cryptomining/#48b90c4d5ae8

[2] https://www.forbes.com/sites/cbovaird/2017/11/17/why-the-crypto-market-has-appreciated-more-than-1200-this-year/#53e14c226eed

Многие компании все еще не имеют полис страхования киберрисков, который обеспечивает возмещение в случае недоступности сети. К примеру, большая часть финансовых убытков в результате атак при помощи программ-вымогателей прошлых лет была отнесена на баланс предприятия (см. таблицу).

Из страховых претензий, полученных в 2018 году, становится ясно, что степень тяжести убытков в результате недоступности сети может значительно отличаться в зависимости от продолжительности инцидента, размера компании и отрасли. При этом потери, возмещенные AIG Europe в связи с недоступностью сети в 2018 году варьируются от 3 250 долларов США до 5,2 млн долларов США.

По словам Хосе Мартинеса, вице-президента по урегулированию крупных финансовых убытков AIG EMEA, страхователи, у которых нет надежной защиты от кибератак или резервного копирования данных, скорее всего, пострадают от недоступности сети в результате атак программ-вымогателей. «Это особенно актуально для малого и среднего бизнеса, так как их системы, как правило, не столь надежны, и зачастую они делают резервное копирование данных лишь периодически», – утверждает он.

«В целом, если у компании есть резервные копии, почти во всех случаях, которые я наблюдал, она не заинтересована платить выкуп», – продолжает он. «Однако в прошлом году было несколько ситуаций, когда это стало настоящей проблемой. Некоторые компании фактически были поставлены на колени, потому что у них отсутствовали необходимые резервные копии. Поэтому, чтобы восстановить информацию, им пришлось рассмотреть вариант оплаты выкупа».

«В подобных случаях, чем дольше продолжается инцидент, тем большие финансовые потери несет клиент», – добавляет он. «Конечно, в 2018, по сравнению с предыдущими годами, было гораздо больше случаев, когда страхователи просили наших партнеров-экспертов из KPMG помочь им справиться с программами-вымогателями, попытаться расшифровать информацию или вернуться к предыдущим резервным копиям. Кроме того, помимо экспертной поддержки, некоторые клиенты подавали заявления о косвенных убытках, связанных с отсутствием доступа к системам и данным, необходимостью отправлять персонал на дом и т.д.».

Риск перерыва в производстве по-прежнему крайне недострахован

Большая часть перерывов в производстве, вызванных программами-вымогателями, шифрующими данные, и другими атаками, которые выводили системы из строя в 2018 году, не была застрахована. Агрессивные действия хакеров с использованием программ-вымогателей не всегда мотивированы получением материальной выгоды, а скорее желанием вызвать дестабилизацию, и финансируются государствами.

Подобная цель была достигнута в больших масштабах, а последствия могли бы быть значительно хуже, если бы WannaCry продолжал распространяться беспрепятственно. В общей сложности на оплату выкупов было потрачено менее 150 000 долларов США, при этом общие экономические убытки, связанные с WannaCry, оцениваются в 8 миллиардов долларов США[3], причем полмиллиарда долларов относится на прямые расходы и косвенный перерыв в производстве[4].

По мере того, как вредоносные программы и программы-вымогатели становятся более изощренными, эксперты ожидают, что убытки, связанные с перерывом в производстве, будут расти. Однако, несмотря на то, что угроза недоступности сети для организаций весьма значительна, она не привлекает должного внимания.

«Когда я вместе с андеррайтерами или брокерами встречаюсь со страхователями, часто они не сильно заинтересованы в покрытии перерыва в производстве, и это странно, ведь сегодня это самая большая проблема для большинства компаний», – говорит Мартин Овертон, специалист по киберрискам AIG EMEA.

«В прошлом году мы наблюдали несколько случаев, когда компании фактически были поставлены на колени, потому что у них отсутствовали необходимые резервные копии». Хосе Мартинес

[3] https://uk.reuters.com/article/uk-cyber-lloyds-report/global-cyber-attack-could-spur-53-billion-in-losses-lloyds-of-london-idUKKBN1A20AH

[4] https://www.jbs.cam.ac.uk/fileadmin/user_upload/research/centres/risk/downloads/crs-cyber-risk-outlook-2018.pdf

GDPR и связанные риски

Мы ожидаем резкий рост претензий, связанных с утечкой данных и другими нарушениями в работе систем безопасности, после вступления в силу GDPR 25 мая 2018 года. Компании будут вынуждены сообщать о нарушениях, а это повлияет на киберубытки подобно тем, что наблюдались в США после введения законов о необходимости подачи уведомлений про утечку данных.

«Многим небольшим страхователям рекомендуют подавать уведомление, но согласно действующему законодательству они не обязаны этого делать», – говорит Эйвери. «После того, как GDPR вступил в силу в мае, такой опции у них не осталось. Поэтому мы, конечно, ожидаем рост количества страховых случаев».

Она отмечает, что после огласки скандала с Cambridge Analytica и Facebook, отношение к персональным данным изменилось. Ожидается, что это повлияет на типы убытков в 2018 году, а в случае утечки персональных данных, потребители будут настроены менее лояльно, чем в прошлом.

«Недавно мы урегулировали претензию в результате утечки данных из университета», – говорит она. «Они подали уведомление в соответствии с требованиями GDPR. Это оказалось довольно дорогостоящим экспериментом, клиенту также было сложно справиться с репутационными вопросами. Когда вы уведомляете 100 000 человек о хищении их данных, сей факт может лавинообразно перерасти в довольно большое дело. Пользователь может негативно воспринять известие о взломе, даже если такое уведомление – лишь предосторожность».

Исход коллективного иска в судах Великобритании против сети супермаркетов Morrisons, предъявленного сотрудниками, станет важным примером того, как суды будут присуждать компенсацию лицам, чьи данные были скомпрометированы. Сотрудники требуют возмещение за моральный ущерб, причиненный хищением персональных данных почти 100 000 человек в 2014 году[5].

Ожидается, что GDPR в будущем приведет к росту судебных исков от акционеров против компаний и их членов правления. В США жесткие требования к уведомлениям уже введены в течение нескольких лет, и почти каждая громкая кибератака заканчивается, по крайней мере, одним коллективным иском.

Хотя в Европе еще нет того же уровня сутяжничества и механизмов коллективного возмещения ущерба, решение по делу Morrisons может послужить примером для предъявления подобных исков в будущем. «Если по делу Morrisons будет принято решение о возмещении морального ущерба в результате утечки данных, это создаст интересный прецедент», – рассуждает Марк Камилло. «Подобное решение может привести к росту аналогичных исков».

[5] https://www.independent.co.uk/news/business/news/morrisons-data-leak-staff-payout-details-sensitive-data-personal-online-hack-a8086521.html

«Большинство договоров страхования ответственности директоров и должностных лиц не исключают иски от акционеров, предъявленные в результате кибератак, поэтому в случае подобных претензий полисы будут применяться», – продолжает он. «Сейчас в отношении GDPR существует много неопределенности, связанной с подходом к штрафам и санкциям. Текущий год может стать первым, когда мы увидим, как применяются эти подходы, в зависимости от того, насколько агрессивными будут регуляторы».

GDPR предусматривает два типа штрафов, которые могут взиматься с компаний за отсутствие необходимых систем и механизмов защиты данных третьих лиц. Первый – до 10 млн евро или 2% от общего оборота за предыдущий год, в зависимости от того, какая из сумм больше. Второй – до 20 млн евро или 4% от оборота за предыдущий год, в зависимости от того, какая из сумм больше.

«Скоро появится определенность, действительно ли подлежат страхованию штрафы и санкции», – говорит Камилло. «Мы уже знаем, что в некоторых странах Европы это будет запрещено. Но в других юрисдикциях, включая Великобританию, ситуация пока не ясна. Правительство сделало ряд заявлений о том, что договоры страхования могут покрывать административные штрафы и санкции».

«Мы знаем, что огромные армии ботнета готовы нанести удар, и нет никаких признаков их замедления». Мартин Овертон

Компании, не сумевшие внедрить защиту от DDoS-атак

Через два года после атаки ботнета Mirai против Dyn DNS, DDoS-уязвимости остаются серьезной угрозой, а компании по-прежнему не принимают достаточных мер для защиты своих сетей от подобных атак.

Ботнет Reaper является новейшей разновидностью. Как и Mirai, он состоит из большого количества незащищенных домашних устройств, которые используют технологии Интернет вещей, включая маршрутизаторы, IP-камеры и радионяни.

«Ботнет Reaper состоит в основном из «умных» устройств, которые могут выдавать более 1,6 терабит в секунду... это очень большой объем данных», – заявляет Овертон. «Мы знаем, что эти огромные армии ботнета готовы нанести удар, и нет никаких признаков их замедления, но у многих компаний до сих пор нет необходимых механизмов защиты».

На рынке есть много решений, гарантирующих работу систем в случае атаки, однако компании не всегда устанавливают защиту от DDoS, а компании малого и среднего бизнеса, вероятно, отпугивают связанные расходы.

Вывод: пришло время проверить свою киберзащиту?

AIG прогнозирует, что существенные финансовые последствия перерывов в производстве/недоступности сетей будут по-прежнему ощущаться на протяжении 2019 года. Это приведет к увеличению спроса на покрытие и постоянному росту рынка киберстрахования в Европе. По мере развития есть ожидание, что частота, а, возможно, и тяжесть этих убытков, будет увеличиваться.

В течение следующих 12 месяцев на страховые случаи по-прежнему будет влиять коммодитизация программ-вымогателей, ожидаемый всплеск убытков, связанных с утечкой данных после введения GDPR, и действия государственных органов на фоне шаткого и политически нестабильного положения. Разумеется, традиционное кибервымогательство и мошенничество с применением имперсонации останутся среди наиболее актуальных тенденций, а сотрудники, как и прежде, будут первой линией обороны от подобных атак.

Независимо от сферы деятельности и масштабов бизнеса, компании, работающие во взаимосвязанном цифровом мире, еще никогда не были настолько подвержены атакам и опасным финансовым последствиям. AIG предполагает, что системный характер взломов данных с применением программ-вымогателей, свидетелями которых мы стали в 2017-2018 годах, – лишь верхушка айсберга, и этот вызов в будущем станет еще более актуальным.

Профилактика всегда лучше лечения, но организации должны быть готовы к тому, что их системы и сети в какой-то момент все же будут взломаны. Киберустойчивые организации – это те, что готовы к подобным событиям и отработали ответные действия в дополнение к надежной стратегии управления киберрисками. У наиболее подготовленных уже есть страховое покрытие, которое обеспечит возмещение на случай различных киберрисков, включая недоступность сети.

ТОП киберугроз для предприятий

Наш опыт показывает, что с точки зрения нарушений в работе систем безопасности, основными угрозами для бизнеса являются:

- Внешние серверы с удаленным доступом в сочетании с ненадежными паролями. Это позволяет внедрить вредоносные программы и программы-вымогатели. Удаленный доступ должен тщательно контролироваться.
- Недостаточная информированность, которая позволяет хакерам получить доступ к паролям при помощи фишинга. Пользователь получает электронное письмо со ссылкой на поддельную страницу, где мошенники пытаются заставить его ввести данные своей учетной записи. Следует задаться вопросом: «Доверяю ли я этому письму?» Любой запрос о предоставлении учетных данных – первый признак возможного фишинга.
- Слабые протоколы входа в систему. Риск фишинга устраняется при помощи двухфакторной аутентификации, которая требует второй код для входа в учетную запись. Как минимум это должно быть реализовано для членов правления и партнеров компании, а также для сотрудников, занимающихся платежами.

Примеры страховых случаев

Производственное предприятие пострадало от перерыва деятельности в результате атаки с использованием программ-вымогателей

Страхователь проектирует и производит краны, экскаваторы, тяжелое и специализированное грузоподъемное оборудование.

1 декабря клиент обнаружил, что стал жертвой атаки с использованием программ-вымогателей. До 85% его папок и документов были зашифрованы. Страхователь позвонил на горячую линию AIG CyberEdge и воспользовался услугой реагирования на инциденты от специализированной ИТ-компании. Следуя рекомендациям, клиент решил восстановить данные с помощью резервных копий. Эти действия были завершены 3 декабря.

В результате отказа ИТ-систем сотрудники разных отделов не могли работать 1 и 2 декабря, так как к серверу не было доступа. Штат страхователя насчитывает около 300 человек производственного персонала и инженеров. Его основная деятельность заключается в реализации проектов «под ключ» или инженерных проектов, где использование ИТ-оборудования имеет большое значение для выполнения работ.

Инженеры хранят данные на сервере компании для обеспечения обмена информацией между сотрудниками. Персонал получает оплату непосредственно за отработанные часы по проекту. Отсутствие у инженеров возможности выполнять работу в течение этого двухдневного периода напрямую повлияло на количество часов, за которые компания могла бы выставить счет. Трудно наверстать эти часы позже, потому что у страхователя по различным проектам уже были согласованы сроки. Несоблюдение сроков привело бы к применению штрафных санкций со стороны клиентов.

AIG предоставила покрытие дополнительных расходов на услуги инженеров, чтобы гарантировать непрерывность работы и своевременное завершение проектов.

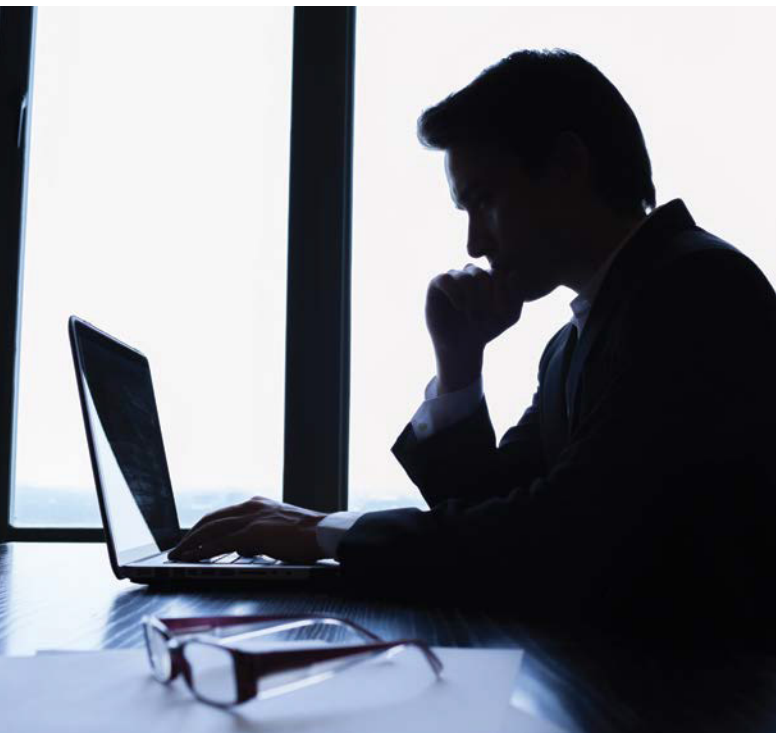
Финансовое учреждение под угрозой DDoS-атаки и вымогательства

Застрахованная компания получила электронное письмо с требованием выкупа на сумму в один биткойн, иначе злоумышленники начнут DDoS-атаку против страхователя. Если выкуп не будет уплачен, они также пригрозили увеличить сумму до десяти биткойнов.

При содействии AIG страхователь подключил службу защиты от DDoS-атак для смягчения последствий и уведомил своего провайдера о возможной попытке атаки вместо того, чтобы самостоятельно урегулировать ситуацию при помощи собственных ограниченных ресурсов, таких как брандмауэры.

В результате расследования выяснилось, что потенциальные хакеры находятся в Латвии. Злоумышленники заявили, что они – XMR Squad, которые за последние недели провели DDoS-атаки против нескольких компаний, и, следовательно, представляли реальную угрозу. Однако информация, полученная от Банка Англии (центрального банка Соединенного королевства), указывала на то, что письмо, скорее всего, пришло от подражателей, а не от настоящей хак-группы.

Не было никаких подтверждений того, что преступники получили доступ к персональным данным, контролируемым страхователем. В конечном итоге угроза не оправдалась, никакого негативного влияния на конфиденциальность, целостность или доступность информационных активов страхователя не было.



Веб-сайт и цифровая платформа нашего клиента продолжили работать, правда, был обеспечен усиленный мониторинг и анализ трафика. Компания не пострадала от серьезных финансовых убытков, за исключением расходов, связанных с внешними юридическими и другими консультациями по вопросам управления кризисными ситуациями и подобными инцидентами, а также большим количеством времени на расследование и разрешение ситуации. Расходы по реагированию на инцидент были покрыты AIG.

Направленная фишинговая атака на производителя предметов роскоши

Застрахованная компания стала жертвой мошенничества с использованием фишинговой рассылки электронных писем, направленных вначале на сотрудников, а затем на клиентов.

Предварительное расследование показало, что сотрудник перешел по ссылке из фишингового письма, еще за девять месяцев до того, как страхователь узнал о каких-либо проблемах, тем самым предоставив доступ злоумышленникам к своей почте. По крайней мере еще два почтовых ящика других сотрудников были взломаны, когда те перешли по ссылке из аналогичных фишинговых писем. Получив доступ к трем почтовым ящикам, преступники могли завладеть контактной информацией клиентов.

В течение последующих 12 месяцев и с растущей частотой страхователь начал получать уведомления от клиентов о поддельных фишинговых письмах, имитирующих страхователя, но на самом деле от мошенников. Эти электронные сообщения, как и те, что первоначально получили три сотрудника компании, побуждали клиентов перейти по поддельной ссылке, где им предлагалось ввести учетные данные для входа в систему, информацию о платежной карте и другие персональные данные, используемые для процедуры идентификации клиентов страхователя.

Несколько клиентов, которые сообщили о получении такого фишингового письма, фигурировали в электронной таблице, найденной в одном из почтовых ящиков сотрудника. Это был общий список клиентов с 21 000 адресов электронной почты.

ИТ-эксперты, привлеченные для консультаций со стороны AIG, заблокировали доступ к подозрительному URL-адресу и провели целевое расследование взломанных почтовых ящиков для определения, к какой информации был получен доступ. После глубокого анализа последствия взлома были сужены до менее 1000 записей данных. Это позволило страхователю составить индивидуальную программу ответных действий для пострадавших клиентов, многие из которых были сверхсостоятельными, высокопоставленными лицами.

ВЫПЛАТЫ ПРЕЖДЕ ВСЕГО

Методология

AIG Europe провела анализ более 600 страховых случаев, заявленных по договорам страхования киберрисков в период с 2014 по декабрь 2018 года.

www.aig.com, www.aig.ru

AIG®