AIG®

Можно ли считать кибер-риски системными?

В декабре 2016 года компания AIG провела опрос среди экспертов в области кибер-безопасности и риск-менеджмента, чтобы глубже понять вероятность и возможные последствия системной кибер-атаки.

Несмотря на то, что вопрос ***«Можно ли считать кибер-риски системными?»*** кажется простым, мы считаем, что тут есть множество нюансов. Может ли одна атака затронуть десятки, сотни или даже тысячи организаций одновременно? Будет ли масштаб события обратно пропорциональным его вероятности? Какие отрасли более подвержены системным рискам? Эти и многие другие вопросы стали предметом исследования, представленного в настоящем отчете. Полученные данные будут полезны для оценки системных кибер-рисков и подготовки к атакам. Эти вопросы важны для всех компаний, работающих в кибер-экосистеме. Более того, страховщикам кибер-рисков ответы на эти вопросы необходимы для правильного моделирования и управления аккумуляцией рисков.

Несмотря на то, что вопрос *«Можно ли считать кибер-риски системными?»* кажется простым, мы считаем, что тут есть множество нюансов.

Основные выводы

Однозначное «ДА» – кибер-риски системны

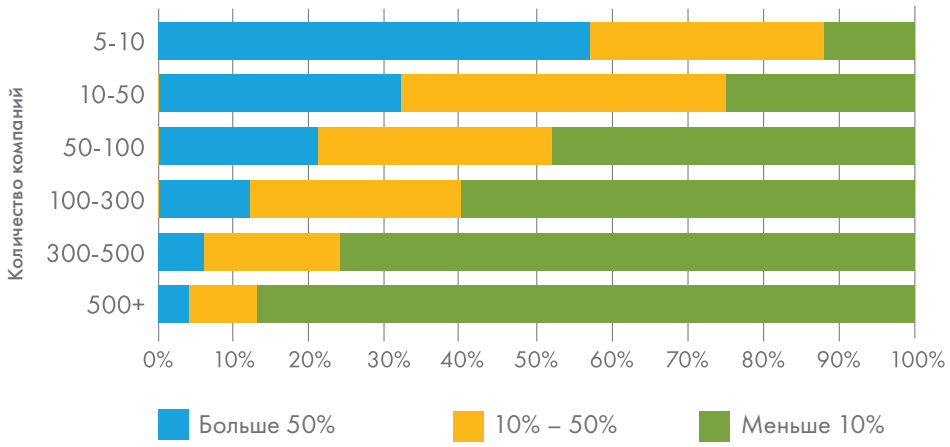
Более 90% респондентов считают, что кибер-риски являются системными, то есть способны одновременно затронуть множество организаций. Такая оценка имеет большое значение для разных сфер деятельности, от кибер-безопасности и страхования до управления рисками. Предприятиям, государственным органам и отдельным лицам необходимо задуматься о своих кибер-уязвимостях, например, при выборе поставщиков, размещении данных в облаке и использовании взаимодействующих устройств и оборудования, которые могут существенно повлиять на степень подверженности рискам. В это же время страховые компании, брокеры и поставщики услуг должны объединиться для усиления физической, виртуальной и финансовой защиты и оказания необходимой поддержки клиентам в смягчении растущих рисков.

Более 90% респондентов считают, что кибер-риски являются системными, то есть способны одновременно затронуть множество организаций.

Как оценить масштаб угрозы?

Определение потенциала системного риска – это первый шаг. При этом важно понять вероятность и последствия системной атаки. Мы попросили респондентов оценить возможность атаки разного масштаба в течение следующих двенадцати месяцев. Подавляющее большинство экспертов считают, что системное кибер-событие, затрагивающее пять-десять компаний, будет более вероятным, чем одновременная атака на 100 или больше компаний. И все же, недавние инциденты, такие как взлом баз данных MongoDB, кибер-атака на Dyn и кража крупных сумм из банковских учреждений через систему SWIFT подчеркивают весьма реальную угрозу масштабных системных событий. В ходе DDoS-атаки на компанию Dyn, под ударом хакеров оказались объекты интернет-инфраструктуры, что вызвало перебои в работе сайтов с большим трафиком из разных отраслей.

Насколько вероятно, что одна системная атака затронет несколько компаний в ближайшие 12 месяцев? (количество = 68)



В конце 2016 и в начале 2017 года хакеры начали кампанию по вымогательству у клиентов популярной системы управления базами данных MongoDB. Предполагается, что злоумышленники воспользовались уязвимостью старых версий, в которых настройки безопасности были установлены по умолчанию. Это упростило доступ, просмотр, редактирование и удаление данных. Эксперты полагают, что во всем мире было взломано от 50 000 до 100 000 баз данных. Согласно оценке компании Flashpoint, специализированной на кибер-безопасности, по меньшей мере 20 000 баз данных были безвозвратно удалены.[1]

По мнению специалистов, исследующих этот вопрос, от атаки пострадали компании разных отраслей, включая здравоохранение, финансовые услуги, образование и туризм.[2] Негативные последствия от потери баз данных трудно оценить количественно, но, вероятно, убытки исчисляются миллионами долларов. Сообщается, что в результате удаления базы данных, одно из известных медицинских учреждений потеряло результаты исследований за три года.

Сфера финансовых услуг под угрозой

Большинство респондентов (85%) считают, что одни отрасли более подвержены системным атакам, чем другие. Сфера финансовых услуг (19%), энергетика (15%), телекоммуникации/коммунальные услуги (14%), здравоохранение (13%) и сектор информационных технологий (12%) оцениваются как наиболее вероятные жертвы системной атаки в следующие двенадцать месяцев. Это дает представление о возможных событиях, свидетелями которых мы можем стать, включая атаки на финансовые сети или системы переводов, объекты интернет-инфраструктуры, энергоснабжения и здравоохранения. Сектор информационных технологий, включая поставщиков программного и аппаратного обеспечения, которые являются основой цифровой экономики, также считаются особенно уязвимыми. Наша высокоинтегрированная экономика опирается на безопасный, слаженный и бесперебойный поток данных и электронные коммуникации. Сбои в работе и взлом данных могут привести к эффекту домино, когда под угрозой окажутся организации, зависимые от информационных технологий.

У вас есть 100 долларов, чтобы сделать ставку. Распределите деньги, исходя из того, какие отрасли, по вашему мнению, пострадают от системной атаки в ближайшие 12 месяцев (количество – 70) (всего распределено 7 000 долларов)

[1] https://krebsonsecurity.com/2017/01/extortionists-wipe-thousands-of-databases-victims-who-pay-up-get-stiffed/#more-375 97
[2] http://www.securityweek.com/33000-databases-fall-mongodb-massacre

Самая большая угроза – массовые DDoS-атаки

На просьбу оценить вероятность наиболее катастрофических сценариев (например, события, затрагивающие 500 или более организаций), респонденты оценили массовую DDoS-атаку на крупного поставщика облачных сервисов как наиболее вероятное межотраслевое катастрофическое событие. Это особенно важно в свете стремительного роста облачных вычислений и популярности устройств Интернета вещей, которые используются для запуска крупных DDoS-атак. Эксперты предполагают, что наиболее вероятными жертвами такой атаки станут компании сферы финансовых услуг, здравоохранения и розничной торговли. Для взлома или уничтожения данных чаще всего используются уязвимости в оборудовании или программном обеспечении, которое широко используется в отрасли.

Атаки на критические объекты инфраструктуры, которые могут привести к значительным человеческим жертвам и телесным повреждениям, оказались наименее вероятными в списке возможных сценариев. Осуществление крупномасштабных атак на объекты инфраструктуры (например, в сфере коммунальных услуг, авиации или перевозок) требует глубокой технической экспертизы, что ограничивает пул потенциальных участников, хотя вероятность этой угрозы все же остается.

Разместите следующие сценарии в порядке от наиболее до наименее вероятного в ближайшие 12 месяцев. Наиболее вероятный = 1, наименее вероятный = 10 (n = 66)	Средняя оценка
Финансовые услуги. 15 взломов. Массовое прерывание деятельности. Массовые DDoS-атаки на финансовые учреждения.	4.1
Здравоохранение. 10 взломов (например, больницы, аптеки, страховые компании). Массовая кража данных. Уязвимости в широко используемом медицинском программном обеспечении.	4.1
Розничная торговля/гостиничный бизнес. 25 взломов. Массовая кража данных. Уязвимости в широко используемом программном обеспечении/оборудовании для обработки платежей.	4.3
Разные отрасли. 350 взломов. Массовое прерывание деятельности. Массовая DDoS-атака на крупных поставщиков облачных сервисов.	4.5
Финансовые услуги. 15 взломов. Массовая кража данных. Уязвимости в широко используемой платежной системе.	4.7
Разные отрасли. 350 взломов. Массовое прерывание деятельности. Уязвимости в широко используемом программном обеспечении (например, Plesk, BIND), работающем под Linux.	6.2
Разные отрасли. 350 взломов. Массовая кража данных. Уязвимости в широко используемом программном обеспечении (например, Plesk, BIND), работающем под Linux.	6.3
Коммунальные услуги/энергетика. 35 поставщиков коммунальных услуг. Массовое прерывание деятельности. Уязвимости в широко используемой автоматизированной системе управления технологическими процессами.	6.3
Коммунальные услуги/энергетика. 10 поставщиков коммунальных услуг. Массовый материальный ущерб, телесные повреждения, прерывание деятельности. Уязвимости в широко используемой автоматизированной системе управления технологическими процессами.	6.8
Авиация. 10 авиакомпаний/аэропортов. Массовый материальный ущерб, телесные повреждения, прерывание деятельности. Уязвимости в программном обеспечении командно-диспетчерских пунктов и бортовых навигационных систем.	8.0

Респонденты оценили массовую DDoS-атаку на крупного поставщика облачных сервисов как наиболее вероятное межотраслевое катастрофическое событие.

Заключение

Научно-технический прогресс двигает общество вперед. Вакцинация, электричество, массовые перевозки и современная химия коренным образом изменили мир к лучшему. Однако с каждым изменением появляется новая угроза и вероятность отклонения от принятых норм. Электронная торговля, возможно, сильнее всего влияет на риски современной экономики.

Как показывают приведенные примеры, рисками можно управлять – большинство респондентов считают, что системные кибер-угрозы можно смягчить при помощи инвестиций в системы безопасности. Наряду с программным обеспечением и оборудованием, необходимо инвестировать в управление и тщательную проверку поставщиков, обучение вопросам безопасности (например, резервное копирование критически важных данных) и страхование для смягчения последствий системной кибер-атаки. Кибер-угрозы будут продолжать развиваться, и средства защиты должны идти в ногу с ними.

Наиболее неблагоприятные сценарии предполагают кибер-войны, атаки на разные отрасли и регионы

Респонденты рассказали о ряде возможных сценариев, которые «пугают их больше всего», от кибер-войн до атак на критические объекты инфраструктуры. Ниже приведены некоторые их таких сценариев:

- Атака на энергосистему, последствия которой скажутся на гражданском населении.
- Кибер-войны, месть и переход к реальным военным действиям.
- Масштабная атака на инфраструктуру телекоммуникаций и коммунальные компании, которая приведет к недоступности базовых услуг.
- Взломы с манипулированием или уничтожением данных (а не кража данных или DDoS-атаки). Изменение медицинских, служебных или финансовых данных, и их недостоверность как результат.
- Использование уязвимостей в защите устройств Интернета вещей критической инфраструктуры, что приведет к крупномасштабным перебоям в работе или телесным повреждениям.

Методология

Для сбора данных в декабре 2016 года компания AIG отправила электронные опросники более чем 100 экспертам по кибер-безопасности, технологиям и страхованию в Соединенных Штатах, Великобритании и континентальной Европе. Среди респондентов были директора по информационной безопасности, специалисты по технологиям и судебные следователи, а также исследователи кибер-рисков, ученые, страховые брокеры, андеррайтеры и специалисты по моделированию рисков.

Контакты

Для получения дополнительной информации о страховании кибер-рисков AIG CyberEdge и об услугах андеррайтинга, урегулирования страховых случаев и предотвращения убытков по продукту AIG CyberEdge, пожалуйста, направьте запрос на reception.moscow@aig.com

www.aig.ru
reception.moscow@aig.com
www.facebook.com/aig.russia
www.twitter.com/aig_russia
8 (800) 700 8950

АО «АИГ»
Лицензии ЦБ РФ СЛ № 3947, СИ № 3947,
ОС № 3947–04, ПС № 3947 от 12 апреля 2017 года
г. Москва, Ленинградский проспект 72/2
©2017 American International Group Inc. Все права защищены

AIG

Созидая будущее