*В последнее время и недели не проходит без сообщений о том или ином киберпреступлении: хакерской атаке на сайт какой-либо компании или взломе личной почты или аккаунта в твиттере мировой знаменитости. Уже первые две недели августа ознаменовались новостями о новых киберпреступлениях. Так, американская компания Hold Security недавно сообщила о самой большой потере данных в истории: группа хакеров украла более 1,2 миллиарда данных и паролей пользователей, взломав более чем 420 тысяч сайтов. Жертвами стали компании совершенно разных отраслей. Вторая же новость – взлом личного микроблога в твиттере премьер-министра России Дмитрия Медведева. При этом неизвестные злоумышленники разместили в нем несколько записей от его имени, включая заявление об отставке.*

Вопрос защиты конфиденциальных и личных данных в интернет-пространстве сейчас стоит как никогда остро. Причем киберпреступники не признают государственных границ, напротив – некоторые виды киберпреступлений (например, DDoS-атаки) в основном имеют трансграничный характер. Опрос, проведенный по заказу международной страховой компании AIG среди риск-, IT-менеджеров, исполнительных лиц и брокеров, которые участвуют в принятии решений по страхованию в частном бизнесе в США и Канаде, свидетельствует: профессионалы ставят киберриски на первое место среди возможных угроз для компании. Именно эту проблему назвали главной 85% участников опроса, придав ей больше значения, чем рискам снижения доходов, нанесения ущерба собственности или инвестиционным потерям.

Российские компании сталкиваются с аналогичными трудностями. Как показывают результаты опроса, проведенного организаторами международного форума по практической безопасности PHDays IV, проходившего в мае 2014 года в Москве, абсолютное большинство российских системообразующих компаний, промышленных предприятий и организаций в 2013 году сталкивались с хакерскими атаками и заражением вредоносным программным обеспечением. В опросе принимали участие представители различных отраслей экономики – банковской, телекоммуникационной, топливно-энергетической, транспортной, а также государственных организаций и ведомств. Согласно полученным данным, в минувшем году инциденты информационной безопасности были зарегистрированы в каждой из 63 компаний, участвующих в исследовании. При этом свыше половины таких инцидентов привели к существенным проблемам: нарушениям доступности внутренней инфраструктуры или сервисов; финансовым потерям, репутационным издержкам, нарушению функционирования IT-инфраструктуры.

Каков же реальный ущерб от киберпреступлений в денежном выражении? В отчете о

тенденциях киберпреступности в 2013 году Cost of Cyber Crime Study, подготовленном специалистами Ponemon Institute при поддержке HP Enterprise Security Products, отмечается: среднегодовой уровень ущерба от кибератак достиг 11,56 млн долларов в пересчете на одну американскую компанию. Показатель оказался на 78% больше, чем 4 года назад, когда был выпущен первый отчет этой серии.

Ущерб российской банковско-финансовой системы от кибератак в 2013 году составил 700 млрд рублей, об этом говорится в обзоре Национальной ассоциации инновационного развития и технологий (НАИРИТ). «Число атак выросло в прошлом году на 112%. На DDoS-атаки (хакерские атаки на вычислительную технику одновременно со многих компьютеров с целью довести ее до отказа) приходится 19,9%, на вредоносное ПО – 16,9%, на фишинговые атаки – 11,9%», – отмечает президент НАИРИТ Ольга Ускова.

По данным НАИРИТ, Института системного анализа РАН и Института социально-экономической модернизации, DDoS-атаки привели к ущербу в российском финансовом секторе в размере 120 млрд рублей. Еще в 150 млрд рублей исследователи оценили репутационные потери организаций финансового сектора. По предварительным данным компании Group-IB, в 2013 году оборот российской киберпреступности вырос приблизительно на 30%. С учетом соответствующего показателя за 2012 год – 1,98 млрд долларов – речь может идти приблизительно о 2,5 млрд долларов.

Существуют ли сегодня совершенные сети, которые невозможно взломать? Этим вопросом задаются службы безопасности компаний всех без исключения отраслей экономики. Согласно прогнозу аналитической фирмы ABI Research, затраты операторов связи, сервис-провайдеров и компаний, занимающихся информационно-телекоммуникационными технологиями, на обеспечение кибербезопасности к 2019 году могут достичь 22 млрд долларов.

Компания TechProResearch провела опрос среди 244 респондентов, представляющих фирмы из различных стран. По словам 41% опрошенных, в 2014 году планируется увеличить долю IT-бюджета, направленную на обеспечение информационной безопасности компаний. В прошлом, 2013 году подобные расходы нарастили лишь 16% фирм, тогда как 11% даже собирались их уменьшить.

Согласно прогнозам аналитического агентства Canalys, к 2017 году мировой рынок

решений для обеспечения информационной безопасности будет в среднем расти на 7% в год, и к концу периода его объем в денежном выражении достигнет $30,1 млрд. Естественно, что первоочередное внимание вопросам информационной безопасности уделяется в банковском секторе. Здесь затраты на информационные технологии вырастут на 4,2% в 2014 году и составят 430 млрд долларов. К 2020 году размер этих инвестиций превысит 500 млрд долларов, прогнозируют аналитики компании IDC.

Хотя компании тратят миллиарды долларов на то, чтобы уберечься от виртуального проникновения злоумышленников, ответ на вопрос об адекватной защите, похоже, остается риторическим. Более того, как отмечают эксперты, в последнее время наблюдается тенденция к технологическому упрощению организации атак, что может привести к дальнейшему росту их количества. Мощность атак ежегодно возрастает на несколько порядков, что существенно затрудняет борьбу с ними. Кроме того, киберпреступники уже редко действуют в одиночку, объединяясь в организации, сходные с террористическими ячейками. Кибератаки в банковской сфере проходят на все более высоком уровне: если раньше целью атак были учетные записи пользователей, то потом мошенники переключились на корпоративные счета, затем на взлом учетных записей сотрудников банков, а теперь нацелились на административные учетные записи, которые могут открыть им доступ к платежным системам организации.

Фактически все это означает, что киберпреступлений избежать невозможно, они будут совершаться и совершенствоваться, а их масштабы будут только нарастать. Но каждая конкретная компания может минимизировать ущерб, наносимый разного рода киберпреступлениями. Конечно, в первую очередь речь идет о серьезной системе технической защиты, и это в принципе правильно. Этот аспект защиты уже давно и усиленно обсуждается в материалах изданий, посвященных вопросам информационных технологий. Однако оптимальное решение должно включать в себя помимо упреждающих средств, еще и средства, помогающие с минимальными потерями пережить уже нанесенный ущерб от киберинцидентов, а также сократить расходы компании на последующее восстановление.

Для этой цели как нельзя кстати подходят специализированные страховые программы. Подобные инструменты обеспечивают структурированную помощь, защиту от финансовых последствий киберпреступлений и от репутационного ущерба, который может понести компания в этом случае. Программа CyberEdge, разработанная международной страховой компанией AIG, относится именно к такому классу.

Она представляет собой специальную программу киберстрахования для обеспечения

информационной защиты персональных и других данных третьих лиц на предприятии от последствий их утечки или незаконного использования. Кроме обязательных покрытий – убытков в связи с нарушениями данных, затрат на расследование и расходы на реагирование – полис также покрывает ряд дополнительных рисков, в частности, перерывы в производстве, вызванные всеми типами кибератак, виртуальное вымогательство и сбои в работе сети по причине киберинцидента.

В случае DDoS-атаки полис покроет расходы на IT-специалистов, которые понадобятся для устранения перерыва в работе сети, а также убытки из-за перерыва в деятельности в связи с недоступностью сети. Если DDoS-атака включала в себя вторжение хакеров в систему, в результате чего и данные, и программы были повреждены, страховая программа возместит стоимость восстановления утраченных данных и/или программ. Немаловажно и то, что предусматриваются также расходы на преодоление репутационных рисков и риска потери клиентов. Наша программа работает на российском рынке полтора года, и многие клиенты AIG уже успели оценить ее на практике.

**Источник: Intelligent Enterprise , 21.08.14**

**Автор: Владимир Кремер, руководитель отдела страхования финансовых рисков ЗАО «АИГ»**