Актуальные угрозы информационной безопасности компании

С развитием современных телекоммуникационных технологий остро проявляются новые проблемы информационной безопасности. Анализ тенденций совершения преступлений с использованием сетей общего пользования позволяет сделать выводы о постоянном росте количества кибератак, совершаемых на Интернет-ресурсы (информация, размещенная на WEB-сайте, WEB-сервер, телекоммуникационная сеть и т.д.). При этом NetWitness подчеркивает, что далеко не всегда за взломом стоят политические интересы и промышленный шпионаж.

Стремительный рост кибератак вызван так же общедоступностью технологий взлома систем компьютерной безопасности, свободный доступ к которым предоставляется в Интернет через социальные сети и хакерские форумы. Например, для осуществления успешного взлома Интернет-ресурсов таких известных компаний как Paramount Pictures и Juniper Networks использовалось программное обеспечение Zeus, свободная версия которого бесплатно распространяется в Интернет.

Результаты исследований авторитетных компаний и агенств, специализирующихся на информационной безопасности говорят о резком увеличении количества кибератак на информационные ресурсы крупных бизнес-структур, а также общественно-политических организаций.

Масштабы глобальной киберэкономики не поддаются точному учету, но согласно предположению распространенному консалтинговой компанией Deloitte, валовой всемирный продукт в сфере хранения и передачи данных с использованием глобальных сетей в 2008 году превысил 70 триллионов долларов.

Как свидетельствуют данные о финансовых оборотах, которые осуществляются посредством телекоммуникационных сетей общего пользования и суммах потерь из-за взломов Интернет-ресурсов, киберпреступность является сферой деятельности, которая приносит большие прибыли ее организаторам. Огромные суммы денег оказываются в карманах преступников в результате отдельных крупных интернет-атак, не говоря уже о небольших суммах, которые не поддаются подсчету.

Согласно новому отчету Symantec, каждую секунду по всему миру хакеры осуществляют более 100 атак на различные компьютеры. По мнению экспертов компании, каждые 4,5 секунды одна такая атака влияет на работу какого-либо компьютера.

В прошлом году компания обнаружила 51% от общего числа идентифицированных за все время ее работы вирусов, троянцев и прочего вредоносного ПО. 2009 г. отметился взрывным ростом числа вирусов – показатели обнаруженных специальных программ на 71% превысили 2008 г. Всего специалисты Symantec обнаружили за год почти 2,9 млн образцов вредоносного кода.

Также Symantec опубликовал результаты своего глобального исследования корпоративной безопасности. Исследование проводилось в январе 2010 г. В опросе участвовало 2100 представителей компаний – IT-директоров, руководителей управлений информационной безопасностью и IT-менеджеров из 27 стран.

Исследование показало, что многие компании считают обеспечение информационной безопасности одной из ключевых задач. Результаты не стали неожиданностью, поскольку за последние 12 месяцев кибератакам подверглись до 75% опрошенных организаций. Подобные атаки обходятся компаниям в среднем по 2 миллиона долларов в год.

В ключевых аспектах исследования в частности отмечалось:

– глобальные корпорации сильно обеспокоены вопросами безопасности: 42% компаний называют киберриски своей главной проблемой, которая волнует больше, чем стихийные бедствия, терроризм и традиционные преступления в целом;

– компании переживают частые атаки: 36% компаний определили атаки как весьма результативные для злоумышленников. Более того, 29% опрошенных заявили, что в течение прошлых 12 месяцев атаки участились;

– каждая опрошенная компания в 2009 году потерпела ущерб из-за кибератак. Основные три направления атак, по мнению опрошенных – это кража интеллектуальной собственности, кража финансовой информации клиента или данных его кредитной карты или кража личных идентификационных данных клиента;

– потери вызванные кибератаками, оборачиваются денежными затратами в 92% случаев. Основные затраты – это снижение производительности, дохода и клиентского доверия.

Как показывают результаты многих исследования – большинство компаний уделяют гораздо больше внимания защите от внешних атак, тем самым обходя вниманием не менее частые и потенциально более разрушительные случаи внутренних инцидентов.

Информационный бюллетень IDC «Управление внутренними рисками: общий подход к обеспечению внутренней безопасности», посвященный вопросам потенциальных внутренних рисков, которые исходят от сотрудников, имеющих доступ к критически важным системам и конфиденциальной информации, свидетельствует о том, что хотя руководители осознают существование таких рисков, забота о внешних угрозах информационной безопасности часто перевешивает остальные вопросы. Исследование, в котором принимало участие 400 руководителей крупнейших компаний из области ИТ, показало насколько мало внимания уделяется вопросам защиты от внутренних угроз при значительном количестве нарушений – случаев несанкционированного доступа и использования корпоративных информационных ресурсов самими сотрудниками, что ставит под угрозу основу бизнеса многих компаний.

Новый отчет посвящен внутренним угрозам, т.е. угрозам потери корпоративной информации по вине самих сотрудников. В документе, подготовленном по результатам опроса более 2000 сотрудников и ИТ-специалистов из Австралии, Бразилии, Великобритании, Германии, Индии, Италии, Китая, США, Франции и Японии, сопоставляются озабоченность ИТ-профессионалов по поводу такого рода угроз и реальные поступки сотрудников, которые – случайно или умышленно- могут подорвать престиж компании и нанести ей колоссальный ущерб.

Один из самых примечательных результатов проведенного исследования состоит в том, что большинство ИТ-специалистов почему-то считают, что остальные сотрудники компании все лучше понимают риски в области информационной безопасности и все старательнее защищают корпоративные данные. Между тем, опросы самих сотрудников говорят совсем о другом, заставляя более трезво взглянуть на истинное положение вещей. Исследование также показало, что внутренние угрозы, то есть случайное или преднамеренное разглашение корпоративной информации самими сотрудниками, могут нанести компании не меньший ущерб, чем атака извне.

Ситуация с кибератаками на Интернет-ресурсы в Украине в последние годы набирает новых оборотов, что вызвано, также ростом использования глобальных сетей в корпоративной деятельности и общественной жизни украинского социума.

Так, конец августа 2009 г., в Украине ознаменовался самой крупной за всю историю Уанета DDOS-атакой, которая характеризовалась массированным использованием заражен-

ных компьютеров, находящихся в Украине. Цель атаки: автономная система 28 907 (Imena.UA/MiroHost.net). По словам технического администратора украинской сети обмена трафиком UA-IX Сергея Полищука, на пике атаки инфраструктура провайдера испытывала нагрузку в 2 Гбит/с и более.

Впервые, совместными усилиями нескольких украинских компаний, удалось определить два IP-адреса, указывающих на центр управления бот-сетью, ассоциированной со спамерским провайдером Real Host Ltd, владеющим частью крупнейшей в мире бот-сети Zeus (по некоторым оценкам, она состоит из 3.6 млн компьютеров).

Эксперты считают, что эта DDOS-атака является «первой ласточкой» своего рода тренировочной атакой, проверкой на прочность всех систем сетевой инфраструктуры крупнейших украинских провайдеров. При этом следует обратить внимание на тот факт, что, согласно прогнозам С. Полищука, в течение ближайших двух лет можно ожидать повышения уровня объемов DDOS-атак до 10 Гбит/с и больше.

«К сожалению, у нас DDOS-атаки стали привычным инструментом политической и конкурентной борьбы, который используют для воздействия на неугодные сайты или шантажа электронных магазинов. Зло это общемировое, и Украина здесь далеко не впереди планеты всей. Тем не менее, и в нашей стране в течение ближайших 2-3 лет проблема DDOS-атак приобретет серьезную актуальность и будет требовать соответствующих решений, как от владельцев Интернет-ресурсов, так и от хостинг-провайдеров»,– отметил заместитель председателя правления ИнАУ (Интернет Ассоциации Украины) А. Ольшанский.

Обычно в Украине кибератакам подвергаются интернет-магазины, интернет-казино, крупные информационные ресурсы – проекты, для которых разрыв контакта с пользователями Интернет-ресурсов грозит быстрыми и большими убытками. Так, накануне 8 марта, большинство украинских сайтов, торгующих цветами, подверглись DDOS-атакам, из-за чего стали недоступными для обычных пользователей, в связи с серьезной нагрузкой на каналы передачи данных этих ресурсов, и соответственно понесли весомый материальный ущерб.

Как констатирует А.Ольшанский, сегодня оборот денежных средств Уанет оценивается в 10-20 млн. долларов в год и стремительно растет, поэтому и материальные потери спровоцированные несовершенством или во многих случаях отсутствием систем защиты информационных ресурсов также возрастут. Пример тому наша соседка Россия, которая сегодня столкнулась с угрожающими масштабами киберпреступности. Так, например, с начала 2004 г. зафиксировано около 5000 попыток атак на информационные системы и телекоммуникационные сети ОАО «Российские железные дороги», убыток от которых мог составить около 1 млрд. руб.

На сегодняшний день уровень защищенности украинских Интернет-ресурсов, от разного рода интернет-атак из телекоммуникационных сетей общего пользования, характеризуется как не значительный. Но приведенные выше примеры свидетельствуют о росте в недалеком будущем количества кибератак и их масштабности, что повлечет за собой серьезные материальные потери владельцев Интернет-ресурсов и телекоммуникационных сетей.

В Украине затраты на обеспечение информационной безопасности Интернет-ресурсов не соизмеримы с постоянно растущими потерями из-за отсутствия применения комплексного подхода к внедрению средств и методов защиты для закрытия внутренних каналов утечки информации и защиты от атак из внешних источников. Это вызвано в ряде случаев не достаточной осведомленностью владельцев информационных ресурсов о перспективах применения комплексной системы защиты информации (КСЗИ).

С внедрением все большего числа современных интернет-технологий в деятельность украинских бизнес-структур остро проявляются новые проблемы информационной безопасности и не готовность украинских Интернет-ресурсов совладать с масштабами мировых киберугроз. Как гласит украинская пословица: «Доки грім не гряне, мужик не перехреститься».

Предупредительные действия всегда эффективнее и менее затратные, чем меры направленные на устранение последствий кибератак и восстановления работоспособности Интернет-ресурсов. Применение эффективной стратегии информационной безопасности с акцентом на предотвращение проблем поможет избежать материальных потерь в будущем.

Современный рынок услуг в сфере информационной безопасности предлагает массу аппаратных, аппаратно-программных и программных решений способных обеспечить необходимый уровень безопасности информационных ресурсов. Главными условиями являются – выбор оптимального решения, согласно угрозам информационным ресурсам и возможным материальным потерям в связи с их реализацией, правильное и профессиональное выполнение настроек средств защиты информации, а также внедрение необходимых организационных мер для закрытия внутренних каналов утечки информационных ресурсов, представляющих ценность для их владельцев.

Компания, которая обладает комплексным решением, рядом продуктов и услуг, которые обеспечивают круглосуточную защиту, поиск угроз и реакцию на них, сможет избежать многих рисков связанных с угрозами ее информационной безопасности. Такой поход является более рентабельным, чем восстановление безопасности сети после того как она была скомпрометирована.

Согласно приведенной статистике и мнений ведущих экспертов в области ИТ можно сделать вывод, что наличие процветающего хакерского сообщества, конкурентной и политической борьбы, которая все больше использует киберпространство для ведения кибервоин, предвещает лавину новых хитроумных кибератак на информационные ресурсы и телекоммуникационные сети.

Компания «Арт-мастер» с 2006 года занимается предоставлением услуг в сфере информационной безопасности: построением КСЗИ корпоративных сетей передачи данных и Интернет-ресурсов, аудитом информационной безопасности и т.д. За этот период было построено и внедрено более 20 КСЗИ автоматизированных систем различных классов, основная часть из которых большие распределенные системы. А также обеспечивает сопровождение КСЗИ и их модернизацию согласно новым требованиям и угрозам.

Если Вам есть, что защищать – будьте бдительны.

Павленко Елена
Специалист по технической защите информации в компьютерных системах ООО «Арт-мастер»