Безопасность – дело профессионалов

По статистике, хакерские атаки на компьютеры простых пользователей и компаний столь часты, что стали настоящим бичом современности. Впрочем, противостоять угрозам можно, если использовать надежные системы сетевой безопасности, считают эксперты в области ИТ.

Как правило, за исключением случаев атак на известные мировые компании или государственные ведомства вроде американского Пентагона, бесчисленные попытки взлома или кражи данных остаются вне поля зрения массмедиа. Однако ущерб, который киберзлоумышленники наносят рядовым гражданам и коммерческим компаниям просто огромен.

По данным отчета Norton Cybercrime Report 2012, опубликованного антивирусной компанией Symantec, ущерб от кибератак исчисляется в миллиардах долларов. Согласно этому отчету в 2012 году в мире от действий хакеров пострадало 556 млн человек, каждому из которых был нанесен ущерб на сумму порядка $200. К сожалению, Казахстан также не избежал этой участи, пополнив печальную статистику в виде пострадавших граждан и целых компаний.

При этом по вполне понятным причинам наибольший интерес для злоумышленников представляют не частные лица, а именно сети и базы данных ряда компаний. Всего несколько минут достаточно хакеру-профессионалу для получения незаконного доступа к коммерческой информации, разглашение которой просто недопустимо. А так называемые DDoS-атаки способны не только серьезно повредить передаче критически важных данных, передаваемых с помощью IP, но и вызвать полную остановку работы ресурса.

Как отмечают отечественные эксперты, вероятность киберугрозы для компании в первую очередь зависит от степени ее важности на коммерческом рынке. Так, по мнению начальника управления средств технической информации АО «РТРК-Казахстан» Рафаэля Гафарова, если бизнес-логика и рабочие процессы компании напрямую зависят от какого-либо технического интернет-решения, то финансовые потери в результате атак злоумышленников, по сути, обеспечены.

«С развитием интернет-технологий растет потенциал и злоумышленников. Не секрет, что так называемые хакеры весьма неплохие, а порой и просто по-настоящему одаренные специалисты, которые всегда идут в ногу со временем. Соответственно, чем выше, качественнее и современней спектр услуг, предоставляемых компанией, тем актуальней для нее становятся вопросы сетевой безопасности», – считает Р. Гафаров.

При этом, по мнению эксперта, киберугрозы могут исходить не только со стороны казахстанского сегмента сети Интернет, но и от злоумышленников мирового уровня, поскольку, нацеливаясь на повышение эффективности своей работы, большинство предприятий стремится к полной автоматизации рабочих процессов, что делает вероятность попыток несанкционированного доступа к сетям компаний высокой как никогда.

Стоит учитывать и то, что среди других нежелательных последствий таких DDoS-атак может быть снижение заинтересованности в ресурсе ввиду его пусть даже временной недоступности, что зачастую равнозначно упущенной выгоде. В некоторых случаях атаки DDoS выступают в роли отвлекающего маневра, в то время как настоящей целью хакеров может стать конфиденциальная клиентская или корпоративная информация, например номера кредитных карт или объекты интеллектуальной собственности.

Впрочем, все эти риски можно свести к минимуму или даже полностью исключить путем внед-рения современных ИТ-решений, направленных на обеспечение сетевой безопасности. Однако такой шаг потребует от предприятия серьезных инвестиций, поскольку в случае наличия у компании собственной корпоративной сети понадобятся значительные усилия по установке и настройке всего комплекса необходимого оборудования.

Альтернативой развитию собственных систем защиты может стать аутсорсинг услуг по обеспечению сетевой безопасности. Примером такого подхода, уникальным для стран СНГ, является платформа «Системы предоставления услуг сетевой безопасности» от «Казахтелекома». Особенность системы заключается в том, что для каждого клиента предоставляются свои собственные политики безопасности и защиты. При этом виртуальный межсетевой экран FireWall 24 часа в сутки фильтрует весь входящий и исходящий трафик,

проходящий через систему, а защита от DDoS-атак выявляет любые отклонения и аномалии в профилях клиента, обеспечивая тем самым высокий уровень безопасности сети.

Как рассказал Рафаэль Гафаров, «РТРК-Казахстан» уже давно пользуется услугами АО «Казахтелеком» по обеспечению сетевой безопасности, в частности использует виртуальный межсетевой экран FireWall, что существенно усиливает защиту сети в целом. «Наша компания использует как аппаратные средства защиты, так и программные. Предложенные «Казахтелекомом» решения оказались настолько эффективными, что на сегодня все вопросы, связанные с защитой нашей сети, в том числе контролем и фильтрацией проходящих через нее сетевых пакетов и защиты от DDoS-атак, переданы в подразделение по информационной защите этого оператора», – говорит Р. Гафаров.

Стоит отметить, что с технической точки зрения платформа «Системы предоставления услуг сетевой безопасности» обладает действительно широкими возможностями. По словам Георгия Цекоева, начальника отдела инфокоммуникационных сервисов Дирекции корпоративных продаж АО «Казахтелеком», система способна мгновенно реагировать на самые разные кибератаки. Используя сложную технологию выявления аномалий поведения трафика, она выявляет любую активность, отклоняющуюся от профиля клиента, о чем немедленно уведомляет инженеров оператора и клиента, либо в зависимости от настроек алгоритма действий самостоятельно запускает механизмы фильтрации и очистки от паразитного трафика, отмечает эксперт.

При этом, действуя на основании набора правил, описанных в профилях отдельно для каждого клиента, система также оснащена и функцией адаптивного самообучения. Благодаря этой опции она способна подстраиваться под изменения в активности проходящего трафика, что делает ее гибкой и повышает удобство работы в случае, когда трафик на ресурс клиента органически возрастает.

Впрочем, главное преимущество использования платформы и передачи работ по обеспечению безопасности сети на аутсорсинг, по мнению г-на Цекоева, – это экономический фактор, поскольку клиент избавляется от многочисленных забот и расходов, связанных с приобретением необходимого оборудования и расширением штата. «Оборудование, которое используется для информационной защиты, как правило, весьма специализированное, оно дорого стоит и вместе с тем очень быстро устаревает морально. Кроме того, аппаратной части должна соответствовать и программная, что требует содержания в штате высококвалифицированных специалистов. Именно поэтому услуги по аутсорсингу в сфере ИТ очень востребованы во всем мире», – говорит Г. Цекоев.

Это подтверждает и Рафаэль Гафаров, по его словам, используя платформу «Казахтелекома», «РТРК-Казахстан» серьезно сэкономил на покупке и содержании оборудования стоимостью не один десяток тысяч долларов. Кроме того, предоставляя услуги по аутсорсингу «Казахтелеком» использует самое современное оборудование от уже зарекомендовавших себя мировых производителей высокотехнологичной техники. «Зная об этом, услугам этого оператора начинаешь доверять еще больше», – делится г-н Гафаров.

Учитывая, что сегодня все больше казахстанских организаций и компаний развивают собственные сети и включаются в электронный бизнес, популярность аутсорсинга в сфере сетевой защиты в Казахстане, очевидно, будет возрастать. Высокий уровень защиты, отказоустойчивость и круглосуточная техническая поддержка системы, наряду с доступной стоимостью услуг по аутсорсингу, услуг по обеспечению безопасности, делают платформу «Системы предоставления услуг сетевой безопасности» от «Казахтелекома» выгодной альтернативой немалым капитальным и оперативным затратам на создание собственной службы информационной защиты.

Автор: Арман Бурханов 17-10-2013

http://www.kursiv.kz/news/details/vlast1/Bezopasnost-delo-professionalov/