Искусство быть сильнее врага

«Желая мира –
готовься к войне»
(Никколо Макиавелли)

Эти слова средневекового итальянского философа-мыслителя и политического деятеля, автора ряда военно-теоретических трудов весьма подходят к нынешней ситуации в мировом виртуальном пространстве, сотрясаемом беспрерывными кибер-войнами всех со всеми.

Ибо для организации на информационную систему того либо иного физического, а тем более – юридического лица так называемой DDoS-атаки, чудовищно разрушительного наезда на принадлежащую ему компьютерную сеть, достаточно даже такого пустякового повода, как личная неприязнь некоего имярека к другому имяреку. Либо просто своеобразное представление агрессора о способах развлечений и забав в тенетах Всемирной паутины.

Хотя чаще всего DDoS-атака на чьи-то и особенно корпоративные информационные сети – это чистейшей воды компьютерный терроризм, преследующий цель либо полностью уничтожить бизнес оппонента, либо причинить ему ущерб, несовместимый с возможностями дальнейшего эффективного функционирования.

Кстати, по данным отчёта «Norton Cybercrime Report 2012», опубликованного всемирно известной антивирусной компанией Symantec, вселенский ущерб от кибер-атак, осуществлённых только в прошлом году, исчисляется в миллиардах долларов. При этом количество пользователей Интернет-сетей, пострадавших за этот же период времени от действий хакеров во всем мире, в том числе и в Казахстане, превысило 550 миллионов человек.

Между тем по вполне понятным причинам наибольший интерес для атак виртуальных агрессоров представляют не столько частные лица, сколько информационные сети и базы данных коммерческих компаний различного уровня. За считанные минуты хакеры-профессионалы способны получить незаконный доступ к секретной информации, разглашение которой может повлечь за собой просто катастрофические последствия как для компании, владеющей ею, так и для её партнёров и клиентуры. А так называемые DDoS-атаки в состоянии не только помешать своевременной передаче по назначению некоей критически важной информации, но и вызвать полную остановку работы подвергшегося штурму Интернет-ресурса.

И чем выше уровень компании и её значимость на коммерческом рынке, чем глубже вовлечена её деятельность в Интернет-пространство и теснее привязана к передовым мировым технологиям, тем реальнее вероятность спланированной атаки на её ресурс, тем катастрофичнее могут быть последствия

такого штурма. При этом кибер-угрозы, как известно, не знают границ и могут исходить не только со стороны казахстанского сегмента сети Интернет, но и от злоумышленников мирового уровня, способных штурмовать даже такие виртуальные твердыни, как информационная сеть Пентагона.

И если вы окажетесь не готовыми к отражению подобной виртуальной агрессии, последствия этого могут оказаться ничуть не менее трагическими, чем при военном поражении на поприще реального силового противостояния.

В связи с этим один из известных в Казахстане специалистов по проблемам кибер-безопасности, начальник управления средств технической информации АО «РТРК-Казахстан» Рафаэль Гафаров, считает, что чем выше, качественнее и современнее спектр услуг, предоставляемых компанией клиентам, тем актуальней для неё становятся вопросы сетевой безопасности.

Впрочем, все эти риски можно свести к минимуму или даже полностью исключить путём внедрения современных ИТ-решений, направленных на обеспечение сетевой безопасности. Однако, как считают эксперты, это потребует от предприятия серьёзных инвестиций, поскольку при наличии у компании собственной корпоративной сети понадобятся значительные усилия и средства для приобретения, установки и настройки всего комплекса оборудования, предназначенного для достаточно эффективного отражения кибер-атак извне.

Между тем альтернативой развитию собственных систем виртуальной обороны и одновременно наиболее эффективным решением обеспечения задач сетевой безопасности является защита от DDoS-атак на уровне провайдера связи, участвующего в передаче нуждающегося в зачистке трафика.

Это так называемый аутсорсинг услуг по обеспечению сетевой безопасности со стороны субъекта, располагающего уже в силу своей профессиональной деятельности, компетенции и оснащённости соответствующим оборудованием реальными и эффективными возможностями для защиты трафика широких клиентских масс от несанкционированного вмешательства со стороны.

Платформа «Системы предоставления услуг сетевой безопасности» от АО «Казахтелеком», недавно разработанная и успешно внедряемая этой компанией впервые в Интернет-пространстве стран СНГ, строится на принципах создания для каждого клиента своих собственных индивидуальных систем и политик 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.

Кстати, та же, уже упомянутая выше компания «РТРК-Казахстан» уже давно пользуется услугами Дирекции корпоративных продаж - филиала АО «Казахтелеком» по обеспечению сетевой безопасности с применением виртуального межсетевого экрана FireWall, и здесь очень довольны её высокой эффективностью. По словам Рафаэля Гафарова, предложенные «Казахтелекомом» решения проблем сетевой защиты оказались настолько надёжными, что теперь все вопросы обеспечения сетевой безопасности информационной системы «РТРК-Казахстан» переданы на попечение соответствующего филиала АО «Казахтелеком» – Дирекции корпоративных продаж.

Особенно привлекает корпоративных клиентов способность платформы «Системы предоставления услуг сетевой безопасности» мгновенно адаптироваться ко всем новым угрозам и вызовам враждебного кибер-пространства. Как сказал начальник отдела инфокоммуникационных сервисов Дирекции корпоративных продаж АО «Казахтелеком» Георгий Цекоев, система способна мгновенно и автоматически реагировать на самые разные кибер-атаки. Используя сложную технологию выявления аномалий поведения трафика, она обнаруживает любую активность, отклоняющуюся от профиля клиента, о чём немедленно уведомляет соответствующие службы, либо в случае необходимости самостоятельно запускает механизмы фильтрации и очистки от паразитного трафика.

 При этом действующая на принципах выполнения определённого набора правил, описанных в профилях отдельно для каждого клиента, система так же оснащена и функцией адаптивного самообучения. Благодаря этой опции она способна подстраиваться под любые внезапные изменения в активности проходящего трафика и реагировать на всякое из них соответствующим образом.

Кроме того описанная выше система сетевой защиты славится не только тем, что беспокоится о кибер-безопасности клиента, но печётся и об его кошельке.

Ибо, по словам господина Цекоева, одно из главных преимуществ использования этой платформы с полной передачей функций по обеспечению безопасности Сети на аутсорсинг – это экономический фактор. Ведь клиент полностью избавляется от многочисленных забот и расходов, связанных с приобретением необходимого, часто весьма дорогостоящего и в то же время достаточно быстро морально устаревающего оборудования, его программированием и постоянным поддержанием в боевом состоянии.

Так что, если вы хотите получать максимально надёжную защиту от кибер-агрессоров, затратив на это минимум средств, времени и сил, – то это решение для вас.

Текст: Александр Тонкопрядченко 04.11.2013

http://www.megapolis.kz/art/Iskusstvo_bit_silnee_vraga