"Билайн Бизнес": "Мы защищаем клиентов только в Москве"

["Билайн Бизнес": "Мы защищаем клиентов только в Москве"]Защита от DDoS в "ВымпелКоме" пока реализуется на "автопилоте" - основное решение, которое за последние три года дорабатывалось и улучшалось, все-таки осталось неизменным со времен "Совинтела". Таким оно перешло в "Голден Телеком" и, после приобретения компании, в "ВымпелКом", где его используют время от времени. О будущем подобной системы, подходе к безопасности клиентов и ценах на защиту нам рассказал **Павел Захаров - руководитель департамента маркетинга, развития и управления продуктами фиксированной связи компании «ВымпелКом».**

Схема работы решения

Первая инсталляция Cisco Guard была выполнена в подразделении, которое сейчас принадлежит "ВымпелКому" еще в 2007 году. "Решающим оказался тот факт, что это оборудование можно было легко вставить в шасси Catalyst. При таком подходе победить Cisco вендору, который еще не работает в той или иной компании было крайне сложно", - отмечает Павел Захаров. 2 месяца потребовалось на монтаж оборудования и его доставку, и все заработало к декабрю 2007 года. Проект развивался, и после установки: "Как только решение заработало в полную мощность, стало понятно, что его функциональные возможности надо увеличивать и покупать для этого дополнительную лицензию. Драйвером всего процесса была необходимость защиты как клиентских приложений, так и собственных ресурсов, стоящих в корпоративном ЦОДе, от внешних угроз. Позже началось движение в сторону создания конечной услуги для клиентов, также на основе этого аппаратно-программного комплекса".

Центр очистки у "ВымпелКома" Cisco Guard расположен на одном из основных технических узлов компании в районе метро Авиамоторная в Москве (улица Красноказарменная, где ранее был офис "Голден Телеком"), неподалеку, около ядра сети: здесь установлены и детекторы трафика. Центр очистки подключен параллельно к IP-core. В постоянном режиме защищаются как ресурсы самого оператора связи, так и тех клиентов, которые активировали у себя эту услугу. Весь подобный трафик идет на детекторы, которые "просеивают" его в режиме online. Суммарная пиковая мощность решения - 3 Гбит/с на детектрование и 2 Гбит/с на очистку трафика. "3 года назад этих показателей было более чем достаточно, - говорит Павел Захаров, - на Cisco Guard это считалось максимальными показателями. Сначала мы купили половину этой емкости - 1,5 и 1 Гбит/с соответственно, а потом апгрейд произошел уже с помощью лицензии: железо изначально могло поддерживать все скорости. В настоящее время введено дополнение и к самой системе - организация мониторинга для того, чтобы происходило оперативное оповещение сервис-менеджеров клиентов, которые подключили себе услугу "Защита от DDoS-атак". Большинство атак отбивается в автоматическом режиме, а к пиковым возможностям системы атак подходят не чаще двух раз в год, поэтому отдельного экрана в центре мониторинга, куда было бы выведено общее состояние системы у нас нет – об атаке оповещается конкретный сервис-менеджер клиента".

["Билайн Бизнес": "Мы защищаем клиентов только в Москве"]

В настоящий момент у "ВымпелКома" несколько десятков клиентов, правда, официальные источники расходятся в точных данных. Кто-то говорит, что их "около пятидесяти", кто-то, что всего двадцать. Но сути особенно это не меняет - ясно, что защита от DDoS для компании сервис нишевый. "75% [клиентов] - это банки, 25% крупные корпоративные клиенты, чей бизнес "завязан" на Интернет", - комментирует ситуацию Павел Захаров. Примерно половина компаний, заказавших эту услугу находится в ЦОДе компании в Москве, вторая половина - арендует каналы связи. Типовые скорости, на которых подключены компании - от 10 до 100 Мбит/с (хотя, кто-то "сидит" еще и на 2 и на 5 Мбит/с). 2/3 "подключенцев" приходят без атак «здесь-и-сейчас», но их желание заполучить эту услугу связано с уже случившимся негативным опытом, обычно, недавним. Но чтобы компании часто и массово приходили "под атакой" - такого в "ВымпелКоме" особенно не припоминают: это бывает, но редко.

["Билайн Бизнес": "Мы защищаем клиентов только в Москве"]

К сожалению, несмотря на позиционирование "ВымпелКома" как национального оператора связи, услуга по защите от DDoS доступна только клиентам в Москве. Во всяком случае пока. Между тем, в официальных письменных ответах, которые нам предоставили в дополнение к двум проведенным интервью, было указано, что "используя собственную сеть и узлы связи по всей стране, "ВымпелКом" старается предложить клиентам максимально гибкие варианты защиты от DDoS: от центрального узла очистки трафика до оборудования распределенного по регионам и вынесенного к клиентам". Позиция как минимум двойственная - приходится верить в меньшее.

Стоимость защиты

Ценообразование в "ВымпелКоме" очень интересное. Если клиент только арендует интернет-канал,

то защита от DDoS идет как опция, которая стоит отдельных денег (что вполне разумно и адекватно). Но если клиент находится в ЦОДе компании, то "защита уже включена в стоимость тарифа". Учитывая вышеуказанные цифры о клиентах, это говорит либо о компактном ЦОДе компании, либо о весьма небольшой востребованности этих услуг от оператора в столице. Хотя, более подробно цены указаны в Таблице.
Таблица «Защита от DDoS атак»*.

Порт доступа к сети Интернет находится вне Центра данных Билайн Бизнес						
Скорость порта	2 Мб/с	5 Мб/с	10 Мб/с	20 Мб/с	50 Мб/с	100 Мб/с
Единовременный фиксированный платеж	200	200	200	200	200	200
Ежемесячный фиксированный платеж	250	280	350	450	770	1200

Примечание:*- *тарифы могут быть увеличены, если по результатам технического проектирования для предоставления услуги «защита от DDoS атак» потребуется закупка оборудования под конкретного Клиента, и проект не будет соответствовать принципам окупаемости, принятым в компании.*

"Система обучается в течение рабочей недели, отслеживая пики и спады трафика, и, кроме всего прочего, имеет встроенные профили потребления трафика, которые есть в ее базе данных. Их мы используем для тех клиентов, которые приходят к нам "под атакой". Там уже можно балансировать, указывая каких решений у клиента больше - это "чистый WEB" или клиент-серверные распределенные приложения", - говорит Павел Захаров.

Отдельного SLA для услуги "Защита от DDoS" у компании "ВымпелКом" нет. Качество предоставления сервиса регламентируется договором, заключаемым с клиентом, а доступность услуги составляет 98%. Услуга предоставляется 24 часа в сутки, 7 дней в неделю, время реакции Билайн Бизнес на аварийную заявку клиента - 4 часа в рабочие дни с 9:00-18:00 по местному времени и 8 часов в выходные и праздничные дни.

"В целом, в коммерческую эксплуатацию сервис по защите от DDoS был запущен в конце прошлого года для тех компаний, которые находятся у нас в ЦОДе. А для тех, кто арендует каналы - весной этого года. Между тем, пока что мы особенно его не педалируем, ожидая более современного аппаратно-программного решения", - говорит Павел Захаров.

Как показывает практика, пока что на российском рынке компании, даже крупные, редко осознают, что услуги по защите от DDoS им нудно настраивать и поддерживать в превентивном порядке. Даже интернет-магазины, туристические агентства и банки далеко не всегда считают, что эта услуга из серии первой необходимости. Порой, причем, бывает интересно. "К примеру, недавно мы подключили клиента под атакой, - вспоминает Павел Захаров, - причем, это был чистый DDoS - сайт бомбили запросами. Но после того как мы его поставили под защиту с помощью профиля, который взяли с похожего WEB приложения, атака была устранена на 90-95%, а ресурс стал вполне доступным. Окончательно атака завершилась через пару часов - как только "на том конце повода" убедились, что площадка так просто и без боя не сдастся. А до этого около недели сайт штурмовали потоком "всего" в 500 Мбит/с".

Но, в целом, масштабы атак, имеющих свои цели в Рунете, все же не столь впечатляющи, а десятигигабитные атаки для России пока, к счастью, не характерны. Портрет атакуемой компании в Рунете вряд ли сильно отличается от такового для остального мира: главный признак - это наличие критичного для бизнеса Интернет-ресурса. Под это описание попадает широкий спектр компаний: от интернет-сервиса и интернет-магазина до туристической фирмы и банка.

"Безусловно специалисты отвечающие за "защиту от DDoS" должны обладать глубоким пониманием теории и практики процессов атаки и защиты от нее, но заменить технику по скорости реакции и масштабированию люди не смогут, - говорит Павел Захаров. - В нашей команде работают трое специалистов, которые до этого в течение 5 и более лет занимались развитием и эксплуатацией IP-сетей и клиентских сервисов на их основе в масштабе всей сети Компании". Правда, основную часть времени эти специалисты проводят за "присмотром" за ядром сети, отдельного подразделения по защите именно от DDoS в "ВымпелКоме" нет.

Перспектива на смену

Действующую систему защиты от DDoS в "ВымпелКом" хотят дополнительно "привязать" к управляемым сервисам корпоративной безопасности, наряду с access control, firewall и антивирусными решениями. "Мы планируем, что статистика по загрузке каналов клиента будет собираться и до подключения этой услуги, что позволит ему активировать ее, при желании, практически в режиме online с помощью веб-интерфейса, где он будет управлять и другими своими сервисами", - говорит Павел Захаров.

То есть, по сути, компания хочет работать с рабочими местами, не с сервисом: конкретные услуги не будет подаваться в некоторое облако компании, где они будут обслуживать его самостоятельно, планируется предлагать набор сервисов в расчете на конкретное число рабочих мест. Первая версия такого обновленного продукта будет доступна на рынке уже в конце сентября, правда там такой автоматически настраиваемой защиты от DDoS не будет - скорее, это случится в первой половине 2011 года, надо еще установить новый аппаратно-программный комплекс для этого.

"Когда мы разговаривали по этой теме с сотрудниками российского представительства Cisco этой весной, нам посоветовали брать Arbor, судя по всему, у них есть некое партнерское соглашение с этим производителем. Однако, у нас все-таки будет тендер, куда мы пригласим всех наиболее значимых игроков этого рынка, - уверен Павел Захаров. - Интересно посмотреть не только на массивные аппаратно-программные решения, но и на оборудование от небольших производителей, которые основные деньги делают на аренде приложений: "железо" единообразное, а весь функционал защиты от DDoS открывается различными по стоимости решениями - все похоже на сборку конструктора по кирпичикам. В любом случае, прежде чем мы примем решение о внедрении того или иного решения, оно должно поработать в нашей сети - будут тестовые прогоны и специальная программа испытаний. Нам интересны не только большая, чем сейчас, функциональность, но и развитые презентационные возможности: создание красивых онлайн отчетов, демонстрация статистики, управление. В целом, хочется надеяться, что в этом году мы придем к какому-то короткому списку поставщиков, которых имеет смысл тестировать в условиях реальной сети".

В настоящее время рынок управляемой корпоративной безопасности, куда относятся и решения по защите от DDoS, развит совсем не на том уровне, как бы хотелось основным игрокам. "Если его сравнивать с общим ИТ-рынком - мы пока находимся в стартовой точке, - уверен Павел Захаров, – для чего есть, на мой взгляд, несколько основных причин. Основная - несколько устаревший, но еще очень распространенный взгляд компаний в России на вопросы организации внутренней ИТ инфраструктуры. Многие из ИТ-специалистов не могут себе даже представить, что безопасность компании можно отдать на аутсорсинг - ведь сторонняя компания сможет получить доступ к корпоративной сети. Причем, это можно наблюдать даже на примере такой услуг, как Firewall - компании просто опасаются сторонних поставщиков этой услуги: спокойнее поставить себе конкретное "железо" и самостоятельно его настроить. Поэтому часто встречается мнение, что лучше в этой области работать своими силами. К тому же, с точки зрения конкретного ИТ подразделения – это, казалось бы, гарантированная занятость на многие годы вперед. Но в реальности - для компании это только лишние расходы, а для ИТ подразделения – риск оказаться «за бортом», если такая инициатива придет «сверху». Ведь наиболее убедительный аргумент, второй после надежности, - это очевидный финансовый эффект: экономия на некоторых управляемых сервисах типа IPVPN составляет порядка 40-50%. Преимущество же на рынке и наибольшую долю контрактов будет иметь именно та компания, которая сможет победить сложившееся недоверие к аутсорсингу".