КТО В ОТВЕТЕ ЗА БЕЗОПАСНЫЙ ИНТЕРНЕТ?

Современный джентльменский набор пользователя, решившего обеспечить безопасность при работе с компьютером, может выглядеть примерно так: персональный антивирус, персональный межсетевой экран, антиспам для почтового клиента, контентный URL-фильтр, антифишинговое решение[1].

Разрабатываемые на начальном этапе своего развития антивирусные средства были сравнительно просты, однако по мере "взросления" программного обеспечения в целом и вирусов в частности разработчикам приходилось усложнять свои продукты, добавляя новые барьеры для защиты от вредоносного кода. Сегодня фокус сместился в сторону комплексных решений, включающих антиспам, персональные межсетевые экраны и даже URL-фильтр.

Настройка каждого из этих компонентов является, пожалуй, основным этапом защиты компьютера. От выбранной области сканирования антивируса зависит его эффективность и нагрузка на компьютер. Уровень детектирования спам-пи-сем влияет на процент ложных срабатываний, то есть на количество писем, ошибочно принятых за нежелательные. Правильная настройка межсетевого экрана -задача, требующая серьезных знаний и навыков. К сожалению, разработчики не в силах предустановить все необходимые правила по фильтрации сетевых соединений заранее: слишком много вариантов подключения к сети и огромное количество приложений, обращающихся в сеть, не позволяют сделать этого. Чаще всего эти решения настраиваются методом обучения, когда каждый раз при обращении в сеть нового приложения пользователю предлагается принять решение: разрешить эту активность или нет? Понятно, что чаще всего пользователи выбирают ответ "yes". Логика достаточно проста: я запускаю приложение, а мой файервол на него "ругается", но ведь это я его запустил, значит, надо разрешить. О том факте, что запускаемое приложение, например, может быть инфицировано трояном, мало кто задумывается. После недели таких "настроек" все шпионы и агенты ботнет-сетей комфортно чувствуют себя на рабочем месте пользователя, прекрасно уживаясь с установленными средствами защиты. Пользователь, желающий максимально повысить безопасность ПК, может предпочесть использовать перечисленные выше решения от разных вендоров - выбрать лучшее приложение в каждом классе. Правильный по своей сути подход на практике приводит к еще большему количеству настроек (ведь у каждого приложения свой собственный интерфейс), а также требует дополнительного внимания в части своевременного обновления программ и актуальности подписки (при использовании платных продуктов).

ЛИЦОМ К КЛИЕНТУ

Понятно, что основным источником угроз безопасности персонального компьютера была и остается сеть Интернет. Эпоха создания вредоносного кода с целью потешить свое самолюбие или прославиться давно прошла. Злоумышленников не интересуют компьютеры, не подключенные к сети, в силу того, что их нельзя эксплуатировать удаленно. Современные вирусы - это эффективный способ зарабатывания денег: зараженный компьютер может стать источником рассылки спама или участником заказной DDOS-атаки (распределенной атаки типа "отказ в обслуживании"), наконец, вычислительные мощности подконтрольного компьютера можно просто продать или использовать в своих целях (взлом пароля, расшифрование защищенных финансовых транзакций и т.п.). Для эксплуатации зараженного компьютера во всех этих случаях надо иметь возможность подключиться к нему через сеть Интернет.

Коль скоро основная угроза исходит со стороны Всемирной паутины, то и помощь было бы логично ожидать со стороны тех, кто предоставляет доступ в сеть, то есть Интернет-провайдеров. И такие услуги постепенно отвоевывают свой рыночный сегмент. Крупные и не очень, региональные и федеральные , все большее число провайдеров становятся дистрибьюторами средств персональной защиты (антивирусы, межсетевые экраны и т.п.). Пользователям гораздо удобнее скачать антивирус с сайта провайдера и оплатить со своего счета ключ

[1] Последние два пункта обычно реализуются в виде плагинов (надстроек) к браузеру.

активации, причем зачастую по выгодной цене. Ходить в магазин не нужно, испытывать муки выбора тоже (провайдер этот выбор уже сделал, обычно это 2-3 предложения от различных антивирусных вендоров), даже следить за окончанием срока подписки на обновления не надо - необходимая сумма может автоматически списываться со счета абонента. Кстати, скачивание обновлений обычно тоже бесплатное (с точки зрения оплаты трафика), поскольку осуществляется с локальных серверов провайдера. Все, что требуется от пользователя, - вовремя вносить абонентскую плату.

Пользователь доволен - экономия денег и времени налицо, антивирусный вендор счастлив - его клиентская база растет, да и провайдер не внакладе. Эту идеалистическую картину портит единственный факт: способ приобретения персональных средств защиты никак не влияет на их эффективность.

НЕ ВСЕ ПРОВАЙДЕРЫ ОДИНАКОВЫ

Подключение к сети Интернет - это востребованная услуга оператора и осознанная необходимость для большинства современных людей. Вместе с тем этот вид услуг пока слишком далек от принципа "все включено", и ситуация напоминает скорее стихийный рынок на городской площади, нежели современный гипер-маркет, ориентированный на потребителя.

Простая аналогия: представим себе горную экскурсию. Гид за определенную плату показывает красоты местного края и рассказывает туристам об истории и значении каждого камня вокруг. Туристы ходят, смотрят, фотографируют. Их водят по дорогам, на которых расставлены специальные оградительные знаки, они прошли инструктаж по технике безопасности, гид обходит стороной опасные обрывы и избегает маршрутов, где есть риск камнепада. Это один вариант. Второй: туристы покупают билеты на горную экскурсию, им говорят "вам туда", а дальше каждый предоставлен сам себе. Есть риск? Есть.

Подключение к сети Интернет пользователя, не сведущего в вопросах информационной безопасности и защиты своего ПК, сродни выходу неподготовленного туриста на горный маршрут. Для сведения риска к минимуму в походе нужны профессиональные гиды и соответствующее снаряжение. Следуя этой логике, мы приходим к тому, что услуга обеспечения безопасности при работе домашнего пользователя или компании с Интернет-ресурсами есть сфера ответственности Интернет-провайдера.

Действительно, наличие специалистов, узкая специализация в области защиты от постоянно прогрессирующих Web-угроз, собственная инфраструктура и имеющиеся серверные вычислительные мощности - всего этого нет в арсенале домашнего пользователя. Между тем для достижения приемлемого результата в обеспечении безопасной работы в Интернете система защиты должна быть как минимум грамотно инсталлирована и настроена. Обязаны ли родители разбираться в настройках файервола и думать о безопасном использовании собственным ребенком общего компьютера с выходом в Интернет? Под силу ли это любому среднестатистическому пользователю? И что ему вообще нужно, этому пользователю? Не думать о Web-угрозах и иметь гарантии безопасности при посещении любых сайтов. Другими словами, пользователю нужен чистый трафик, поступающий на его компьютер, а не набор продуктов, пусть даже по очень выгодной цене.

БЕЗОПАСНЫЙ ИНТЕРНЕТ. ОБЩИЕ КРИТЕРИИ

Предоставление провайдерами услуг безопасности как сервиса требует внедрения соответствующих технологий. Понятно, что установка на сервер персонального межсетевого экрана или антивируса - это не метод, нужны специальные шлюзовые решения. Именно здесь скрывается подводный камень. По сути, антивирус большую часть своего развития был персональным, и подавляющее большинство современных шлюзовых решений выросли из персональных.

Адаптация продукта, годами разрабатываемого как персональное средство, для решения несвойственных ему задач, - это скорее маркетинг, чем инновационная технологическая идея. Сделать на платформе "Оки" грузовой автомобиль, наверное, можно, но только зачем?

Вместе с тем на мировом рынке представлен целый ряд решений, изначально проектируемых как шлюзовые системы контентной фильтрации, способные анализировать Web-трафик для неограниченного количества одновременно работающих абонентов. Примеров таких решений на российском рынке несоизмеримо меньше. Тем не менее, попробуем проанализировать критерии, которым должны удовлетворять решения операторского класса для обеспечения безопасной работы абонентов с Интернет-ресурсами.

Во-первых, это неограниченная масштабируемость, благодаря которой установленное на оборудовании оператора решение способно обеспечивать безопасный Web-серфинг для сколь угодно большого количества одновременных сессий.

Во-вторых, бесклиентская модель работы, то есть реализация популярной сегодня концепции SaaS (Secure as a Service) в чистом виде. Решения операторского класса не требуют установки клиентского программного обеспечения на компьютере абонента, что исключает риск некорректной инсталляции и настройки системы безопасности. Доставляя пользователю контент, прошедший многоуровневую систему фильтрации, они создают защиту от проникновения вредоносного кода, блокируют неавторизованные приложения и осуществляют фильтрацию как входящего, так и исходящего трафика на уровне сетевого шлюза провайдера без внесения заметных замедлений и увеличения нагрузки на аппаратные ресурсы ПК абонентов.

В-третьих, это возможность формирования различных пакетов услуг как для домашних абонентов, так и для организаций. Такие решения призваны повысить конкурентоспособность провайдера, благодаря включению в его портфель спектра новых услуг защиты от угроз со стороны Интернета ("Чистый Интернет") и URL-фильтрации ("Родительский контроль").

Как правило, услуги для физических лиц предполагают очистку Web-трафика, передаваемого по протоколам HTTP и FTP. Если заражение уже произошло, абонент автоматически перенаправляется на заданную Web-страницу для очистки ПК от вредоносного кода. Блокирование доступа к сайтам, которые содержат информацию, неприемлемую для детей и подростков, обычно входит в пакет услуг "Родительский контроль". Защита от вредоносного спама производится на основе фильтрации почтового трафика по протоколам SMTP/POP3 с минимальным количеством ложных срабатываний, чему разработчики комплексов для ISP уделяют пристальное внимание.

Услуга "Чистый Интернет" для корпоративного использования предлагает фильтрацию всего потока Web-трафика по протоколам HTTP, HTTPS, FTP. Кроме того, сервис содержит возможность URL-фильтрации, то есть управления доступом сотрудников к сайтам на основе принадлежности ресурса к той или иной категории. Важно отметить, что работающий на уровне шлюза провайдера кон-тентный фильтр может осуществлять блокирование зашифрованных неавторизованных коммуникаций между компьютерами корпоративной сети и Интернетом. Это серьезное преимущество, которого лишено подавляющее большинство персональных антивирусных средств.