сражения заменят кровопролитные войны преследующие человечество на всем протяжении его развития.

Демин Сергей, РГППУ, ЕГЭМК

гр. 37 ОЭТ

БРАНДМАУЭР

С каждым годом Интернет становится более информативным и доступным, однако в то же время и более опасным. Бурное развитие spyware, adware и прочего вредоносного ПО делает работу в Интернете подчас невозможным занятием, ведь с их помощью за нами не только шпионят, но и могут повредить ПК. К счастью, существуют брандмауэры.

Брандмауэры, или файрволы (firewalls), это программные комплексы, главная задача которых – блокирование несанкционированного доступа из Сети к вашему ПК, а также фильтрация входящего и исходящего трафика. Подобная «двунаправленная» политика имеет очень большое значение, ведь атаки могут происходить как извне (из www или локальной сети), так и изнутри – при попытке вредоносных программ, которые уже попали на ваш ПК, отправить конфиденциальную информацию своему создателю.

Работая над статьей, я просто не мог не рассмотреть интегрированный брандмауэр Windows XP, который автоматически активируется при установке данной ОС. А может, действительно не стоит переплачивать за специализированные утилиты, если те же возможности уже есть в нашем распоряжении, причем совершенно бесплатно? К сожалению, нет, ведь в любой нестандартной ситуации встроенный файрвол Windows не способен хоть на сколь-нибудь адекватные действия. Полный провал по всем leak-тестам, отсутствие контроля исходящего трафика, чрезвычайно примитивная настройка приложений, минимум функциональности – вряд ли это можно назвать удовлетворительным результатом. Впрочем, если вы находитесь в

достаточно защищенной от внешних воздействий корпоративной сети, встроенных средств Windows для работы будет более чем достаточно...

Outpost Firewall

Лучший персональный файрвол не собирается сдавать позиции и сегодня – он становится еще мощнее и удобнее. Приятно, что разработчики Outpost идут в ногу со временем, постоянно внедряя в свои продукты новые технологии. В последней версии произошли следующие обновления: новая версия расширяет спектр контролируемых событий и операций, обеспечивая еще более мощную и более настраиваемую защиту, ограничение доступа к небезопасным сайтам, обеспечивает совместимость с еще более «нагруженными» сайтами, обеспечивая высокую производительность и усиленную безопасность при работе в сети.

У этого брандмауэра огромное количество предустановленных правил для популярных приложений (например, IM-клиента, менеджера загрузки, браузера), что экономит немало времени при конфигурировании файрвола. Отличный модуль контроля компонентов, который теперь стал гораздо «умнее», из-за чего число запросов, требующих реакции пользователя, значительно уменьшилось.

По поводу всплывающих окон и других «прелестях» веб-страничек. Это по плечу нашему гостю – Outpost с легкостью «убивает» баннеры всех видов, а также успешно борется с вредоносными скриптами и подозрительными ActiveX-компонентами браузера. Но в отличие от ZoneAlarm, которая при этом существенно замедляет время загрузки Web-страниц, здесь ничего подобного не наблюдается.

Другая особенность утилиты – возможность подключения дополнительных плагинов, значительно расширяющих ее функциональность. Наибольший интерес представляет модуль WhoEasy. Он позволяет определять по IP-адресу всю доступную информацию о домене, провайдере и даже его адрес.

Что же касается надежности работы и защищенности от атак, то результаты тестов говорят сами за себя. На данный момент Outpost – единственный из существующих брандмауэров, успешно справляющийся абсолютно со всеми тестами на непроницаемость, и выбирая данный продукт, можно быть на 100% уверенным: никто и, ничто не сможет проникнуть в компьютер без вашего на то разрешения. Это, без сомнения, мой выбор.

Kerio Firewall

Еще один популярный файрвол, выгодно отличающийся от лидеров существованием полнофункциональной бесплатной версии. В последнее время авторы брандмауэра взялись за активную доработку. Если раньше Kerio Firewall был практически беззащитен перед новомодными хакерскими утилитами, то сейчас он уверенно блокирует 95% подобных угроз, а значит, подойдет для самого широкого использования. Не в последнюю очередь такой прогресс объясняется внедрением в программу новых функций обнаружения и пресечения WWW-атак, а также более тонких настроек для каждого приложения в отдельности. Не забыты и такие банальные вещи, как блокировка рекламы, всплывающих окон, скриптов, Java-апплетов – в общем, всего, что может помешать комфортной работе во Всемирной Паутине.

Конечно, для полного счастья хотелось бы еще увидеть функцию уничтожения программ-шпионов, но будем надеяться, что авторы вспомнят о ней в новой версии своего продукта. И последний недостаток – непонятный конфликт Kerio Personal Firewall с утилитами для фильтрации содержимого Web-страниц: работу Ad-Muncher она постоянно классифицировала как внешнюю угрозу, и лишь отключив опцию Host Intrusion & Detection System, удалось решить эту проблему. Правда, возникает логичный вопрос: а зачем тогда нам нужен файрвол, если один из его важнейших компонентов будет бездействовать?

ZoneAlarm

Известный конкурент Outpost, а по совместительству – самый популярный брандмауэр на Западе, ZoneAlarm тоже претерпел тотальный апгрейд. Zone Labs распространяет свой продукт сразу в нескольких вариантах: стандартном Pro, расширенном with Antivirus и универсальном ZoneAlarm Suite, где, кроме файрвола, имеются еще антивирус, антиспам- и antispy-ware-утилиты.

Чем подкупает ZoneAlarm, так это легкостью в настройке. При создании нового правила нужно просто активировать опцию «допускать программу XXX к Сети при выполнении аналогичных запросов» – и все, больше она вас не потревожит. Единственный минус – невозможность настройки доступа для каждого порта, IP-адреса и протокола, как это можно сделать в Outpost. Зато с непробиваемостью вашего ПК все будет отлично – теперь ZoneAlarm уже не страшны никакие атаки, и она с честью выходит практически из любой ситуации.

Приятное впечатление оставляют и другие компоненты пакета: антивирус (OEM-версии продукта Computer Associates) и средства защиты конфиденциальной информации. Отдельно стоит упомянуть персональный «сейф» myVAULT для хранения особо важных данных – например о кредитной карточке и паролей доступа к платным WWW-ресурсам. «Закрыв» его, можно не бояться кражи или потери ценной информации – она останется в целости и сохранности в любом случае.

McAfee

Компания McAfee – давний игрок в области сетевой безопасности, и поэтому не странно, что именно она была в числе первых, кто собрал под одной крышей антивирус, файрвол и antispyware-утилиту для наиболее эффективной борьбы с вредоносным ПО. Роль связующего звена исполняет специальный центр управления McAfee Security Center, с помощью которого очень удобно быстро переключаться между различными модулями, а также

своевременно обновлять базы данных антивируса. Однако обратим наше внимание на файрвол, ведь именно он интересует нас в первую очередь.

Весьма порадовала функциональность программы, в частности модуль Traffic Monitor, контролирующий сетевой трафик и ПО, которое его генерирует, а также Trace Viewer, отслеживающий местоположение атакующего по IP-адресу.

Алгоритм создания правил очень прост, и это имеет двоякие последствия: настраивать для программ доступ в Интернет придется лишь один раз, что, безусловно, хорошо, но зато возрастает риск пропустить несанкционированную попытку чужеродного приложения проникнуть в Сеть. И полный провал McAfee Firewall по результатам тестов на непроницаемость – тому печальное подтверждение. Ввиду подобного фиаско даже самые интересные новшества, реализованные в новой версии этого продукта, не способны перевесить чашу весов...

Norton Internet Security

Интересные особенности пакета. Security Inspector – это своеобразный тест ряда критичных для безопасности параметров Windows (в частности, надежности паролей учетных записей, настроек Internet Explorer, а также папок общего доступа и некоторых сервисов Windows). Второй компонент – «надстройка» Norton Protection Center, собирающая информацию от утилит-модулей Internet Security и Norton System Works и своевременно извещающая пользователя о возможных опасностях.

Значительные изменения претерпели и старые элементы пакета: Norton Antivirus стал более эффективно бороться со spyware, блокируя его инсталляцию прямо в процессе установки «зараженного» им ПО, а спам-фильтр AntiSpam научился идентифицировать и уничтожать phishing-письма, широко используемые мошенниками для кражи номеров кредитных карточек. Жаль, что работает он только с Outlook Express и Eudora, о поддержке столь популярного у нас The Bat! и речи не идет.

А вот самый важный компонент NIS – брандмауэр – снова оказался не у дел. Даже смешно становится, когда NIS упрямо игнорирует «дедушек» leak-тестов, которые давно уже внесены в черные списки абсолютно всех файрволов. Говорить о какой-то безопасности после этого просто нет смысла, и единственная надежда на то, что проблемы со spyware и adware возьмут на себя другие утилиты данного пакета.

Дерягин Павел, РГППУ

гр. КТ-204

Руководитель – Толстова Наталья Сергеевна,

доцент кафедры СИС ИнИ РГППУ

НЕЙРОИНФОРМАТИКА И ЕЕ ПРИЛОЖЕНИЯ

Каждый, кто впервые знакомится с нейронными сетями, задает себе вопрос: что такое нейроинформатика? Ответить на него можно по-разному. Можно сказать, что нейроинформатика это способ решения всевозможных задач с помощью искусственных нейронных сетей, реализованных на компьютере. Такой ответ, объясняющий только внутреннюю сущность нейроинформатики, почти никого не удовлетворяет, даже если подробно рассказывать о нейронных сетях, задачах и способах их решения. На самом деле требуется еще определить место нейроинформатики среди других способов решения задач и разобраться, в чем же истинные преимущества нейронных сетей, если таковые существуют?

Термин «искусственные нейронные сети» у многих ассоциируется с фантазиями об андроидах и бунте роботов, о машинах, заменяющих и имитирующих человека. Если переключиться на уровень повседневной работы, то нейронные сети это всего-навсего сети, состоящие из связанных между собой простых элементов формальных нейронов. Большая часть работ