ОБЕСПЕЧЕНИЕ ЗАЩИТЫ РАБОЧИХ СТАНЦИЙ И КОРПОРАТИВНЫХ СЕТЕЙ С ИСПОЛЬЗОВАНИЕМ WINDOWS FIREWALL

В.Л. ЛАЗАРЕВИЧ

Когда дело касается безопасности компьютерных систем, большинство организаций сосредоточивает свои усилия на серверах. Но многие из недавно объявившихся сетевых вирусов, разрушивших целые сети и стоивших компаниям миллионы долларов, нанесли этот огромный ущерб, проникнув в сеть через беззащитные рабочие станции. Злоумышленники – будь то посторонние лица или недовольные сотрудники компании, умеющие контролировать рабочую станцию и имитировать легитимного пользователя системы, могут получать доступ к конфиденциальной информации и ресурсам на локальной системе и в локальной сети. Прошли те времена, когда локальную сеть можно было расценивать как безопасное убежище. Теперь от атак вирусов и действий злоумышленников нужно защищать все рабочие станции.

Очевидно, разработчики Microsoft отдают себе в этом отчет. Именно поэтому в рамках инициативы Trustworthy Computing компания сделала вопрос безопасности ключевым при разработке пакета обновлений Windows XP Service Pack 2 (SP2) — самого крупного ориентированного на безопасность пакета обновлений. Он до отказа набит новыми функциями безопасности для борьбы с вирусами и вредоносными программами, которые могут поражать сети через незащищенные рабочие станции. Самой важной частью SP2 является Windows Firewall — заметно усовершенствованная версия Internet Connection Firewall (ICF). Изменение названия функции отражает тот факт, что Microsoft делает упор на использовании технологии локального брандмауэра для защиты рабочих станций, которые подключены только к внутренней локальной сети, в той же мере, что и для защиты рабочих станций, имеющих подключение к Internet.

По умолчанию Windows Firewall работает в режиме максимальной безопасности и принцип его работы таков — запросы приложений выпускаются наружу, а снаружи принимаются только пакеты, пришедшие в ответ на запросы (соответствие запрос-ответ явно ведется в виде динамической таблицы). Таким образом, при сканировании портов на компьютере с включенным Windows Firewall нет ни одного открытого порта (это логично – пакеты сканера портов не будут пропущены, т.к. их никто не запрашивал). Аналогично дело обстоит с различного рода атаками, основанными на отправке нестандартных пакетов.