

# ATM

## Assurance Technology Management

54 Lanewood Ave.  
Framingham, MA 01701  
Phone (508) 405-0900

info@assurancetech.net      www.assurancetech.net

February 5, 2005

### Microsoft Windows XP Service Pack 2 – ATM's Position

Summary: Windows XP Service Pack 2 should be deployed to all workstations as soon as possible but with the condition that the Internet Firewall component be disabled on all devices that are permanently protected by an existing hardware based firewall appliance. The primary exception will be laptops that may be used on unprotected public networks.

---

Microsoft has been regularly providing updates and fixes to its various operating systems in order to address both technical reliability issues as well as the critically important security issues that are often discovered long after the products have been released. In early September, Microsoft began distributing its second service pack for its Windows XP operating system. This release was unique from all of the previous updates in that not only did it provide fixes for a variety of flaws and security issues, it also incorporated a major change in the way the operating system handles network communications.

Prior to Service Pack 2, the default behavior of all of Microsoft's operating systems was to allow any and all traffic to pass into and out of the computer. These lacks of controls allowed undesirable applications to access the host computer and perform malicious activities on it.

Microsoft's solution was to roll out and activate the "Windows Internet Security Firewall" feature as part of the Service Pack 2 deployment. With the firewall installed, Microsoft altered the default behavior from one which **allows** all traffic to pass in and out of the system to one that **denies** all traffic in and out of the system.

The problem is that in a corporate environment there are quite a number of utilities that need to communicate legitimately with the workstations. Some of these utilities include:

- Symantec AntiVirus Corporate Edition
- Norton Live Update
- Veritas Backup Exec client agent
- The VNC remote control tool
- Dell's OpenManage workstation diagnostics

The important thing to note is that in nearly every instance, the workstations and servers in your offices are already protected from a variety of malicious activities by the Internet firewall appliance installed between your company's network and your Internet service provider. On the other hand, if there is any concern that a device *inside* your network could be the source of a malicious attack, then the Windows Firewall would be an effective measure against this possibility.

At this time, Assurance Technology Management, Inc. has taken steps to prevent the deployment of Service Pack 2 to its client's workstations until sufficient time had passed since its release to allow Microsoft to address initial flaws in the update and to allow the greater computing industry to evaluate the real impact of this radical update.

It is the position of Assurance Technology Management, Inc. that its customers should now proceed with the deployment of Windows XP Service Pack 2 with the condition that the Firewall function be disabled on all devices that are or can be protected by a firewall device. This would include any workstation on home networks that has a suitable router device. The main exception would be those users with laptops that may be traveling and using their systems on an unprotected, public network.

One additional matter to consider is the mechanism used to deliver Service Pack 2 and any future updates to the workstations on your network. Currently this is handled by going to each individual workstation and manually performing the upgrade via the Microsoft Windows Update Website. This method can be very time and bandwidth consuming. As a result, Microsoft is releasing a new utility for managing this process. It will be installed on your server and used to deliver the Service Pack 2 update and any future updates to your network devices. ATM will notify you when we are ready to establish this new service on your network and alert you to any impositions it might have.