

## Article

# Microsoft Learns to Prioritize—Implementing Security Measures at the OS Level

After SoBig and Blaster worms inundated computer systems worldwide, targeting vulnerabilities in the Microsoft systems, Microsoft started to make security one of its priorities. The demand to heighten security at the application level makes sense, as about 90 percent of desktops run Microsoft—meaning if there was a large-scaled cyber attack against this global corporation giant, it could quite possibly result in the failure of the world's computer networks. This worldwide risk compels the need for Microsoft to increase its capabilities in protecting its systems from malicious onslaught. A worldwide failure could seem improbable but the imminent threat of failure to the infrastructure of corporations, big and small, is reason enough for the need of increased security measures.

The recently launched Microsoft Office 2003 suite gave birth to an exciting new feature: the ability for emails and documents to autodestruct. New versions of Outlook, Word, Excel and PowerPoint come with the ability for users to control the usage of the documents they create. Mail messages are protected by encryption, which makes Outlook check with the server to see if the user is allowed to edit, copy or forward the message. In order for the message to be unreadable (“self destruct”) after a certain date, the user can time-stamp the message. Other documents (i.e. Word) can also be encrypted in order to control access. Although documents are deleted, they are not entirely gone from the system. These files continue to reside in various places in the hard drive, which should help public companies in compliance with the Sarbanes-Oxley Act that regulates document management.

The above features may be useful, but only to those who upgrade to Office 2003—another convenient method for Microsoft to ensure a healthy market share for their product. Their dominance in the market is largely due to compatibility issues, although the good news brought by Office 2003 is that the latest versions of its programs are backward-compatible with its predecessors.

While the new features help the communication and preservation of sensitive material, they are by no means the definitive security measures. It is handy at some level but it is still susceptible to indomitable attacks.

Other recent security improvements, apart from those in Office 2003, include reducing the frequency of circulating “non-critical” security alerts from once a week to once a month, allowing more time for end-users to apply a patch. Also, the new Windows operating system will be more efficient in its memory management, which will reduce buffer overflow errors—a problem that enables hackers crack into a system with less effort. Another measure is to make firewalls easier to install for companies. Instead of controlling on an individual basis it could now be centrally controlled.

Having in place these various measures is certainly better than not having any. However, Microsoft is far from perfecting its products in terms of security. The above steps may thwart certain attacks but tenacious hackers will always find their way in. While it may never be impossible for them to breach security, implementing measures that will make life more difficult for these architects of menace is definitely one way to go.

## Sources

- Knight, Will. “Microsoft Offers ‘Self-Destructing’ Documents.” Online posting. 21 Oct. 2003. <http://www.newscientist.com/article.ns?id=dn4295>
- “Microsoft Announces Security Changes in Fight Against Hackers.” 14 Oct. 2003. <http://www.computerweekly.com/Articles/2003/10/13/197866/Microsoftannouncessecuritychangesinfightagainsthackers.htm>
- Wrolstad, Jay “Microsoft Monopoly a Global Security Risk, Experts Say.” Online posting. 24 Sept. 2003. [http://www.newsfactor.com/story.xhtml?story\\_id=22362](http://www.newsfactor.com/story.xhtml?story_id=22362)