Microsoft Ships Baseline Security Analyzer 1.2

WinUpdate 5, Software Update Services 2.0 due out around midyear

By Paula Rooney

CRN –

- 12:11 PM EST Fri., Feb. 06, 2004

As the channel awaits the completion of more secure Windows updates and a patch management server, Microsoft has released an update of its Baseline Security Analyzer that extends scanning to Exchange 2003, Office 2003, Windows 2003 and new languages.

Microsoft Baseline Security Analyzer (MBSA) 1.2, developed with partner Shavlik Technologies and made available last month, is an enhanced utility that scans systems across a network to detect common system misconfigurations and missing security updates for several versions of Windows, as well as Microsoft Java Virtual Machine, MSXML Parser, BizTalk, Commerce Server, Content Management System and Host Integration Server.

The tool--which runs on Windows 2000, XP and 2003--will scan for missing security updates for Windows NT 4.0, Windows 2000, Windows XP, Windows Server 2003, Internet Information Services, SQL Server, Internet Explorer, Windows Media Player and Microsoft Data Access Components, Microsoft said. The utility supports local and remote scanning and features a new graphical or command-line interface to conduct the scans.

The tool is available in French, German and Japanese as well as English. Microsoft licensed Shavlik Technologies' HFNetChk engine for security patch management.

Although the utility will help detect missing security patches, partners and customers are eagerly awaiting the release of Microsoft's next-generation Windows Update 5 hosting service and Software Update Services (SUS) 2.0 server code for in-house patch management use.

Windows Update 5 code is integrated into the Windows XP Service Pack 2, which is in beta testing and due out midyear. SUS 2.0 is expected to move into beta testing this month and ship in May.

Detection tools and patch management solutions can help prevent damage, one security consultant said, noting that one of his Fortune 500 clients has been able to avoid viruses and worms like the recent MyDoom because the company did a full network analysis after the MSBlaster virus.

"Virus-prevention technology is based on a detect-and-prevent model. In order to detect, enterprises need to understand what constitutes normal behavior of their networked business applications, including a comprehensive inventory of the applications that communicate over their TCP/IP networks," said Adam Lipson, president and CEO of Network and Security Technologies, Pearl River, N.Y.

"This past Monday evening, that same client began seeing excessive traffic on TCP port 3172," Lipson said. "They looked in the application port inventory that we had created for them. They noted that activity on port 3127 was not associated with any operating system, off-the-shelf package or custom business application. Because they understood the normal behavior of their networked business applications, they were able to shut down traffic on port 3172, thus stopping the MYDoom virus, while being assured that they would not impact any required business application."

MBSA 1.2 is available for download at www.microsoft.com/mbsa.