

enterprise week

Editor: Eamonn Sullivan

THE IT AT THE HEART OF YOUR BUSINESS

Viruses outsmart security

EAMONN SULLIVAN

Corporate IT managers have so far encountered over 20 permutations of the Love Letter virus, a worm that has once again exposed vulnerabilities in the Windows platform and showed that antivirus software, by itself, may not be enough to combat future threats.

IT managers looking to make Windows more secure have several choices, including working through long checklists of registry and file permission changes on Microsoft's Web site. But the list prompted some to question why Microsoft does not ship Windows in a more secure state.

"Windows is shipped with too many services turned on by default," said Winn Schwartau, chief executive of Security Experts, a Florida-based security consultancy.

But Microsoft defended its security stance. "You can either take the approach of locking it down and allowing administrators to open it up, or deliver it open and give people the ability to lock it down," said Peter Birch, architectural systems engineer with Microsoft. "But if we locked it down,

- CHECKLIST FOR WINDOWS SECURITY**
- Visit Microsoft's security site and disable or remove unnecessary features and services from both servers and desktops.
 - Sign up for security alert email lists.
 - Install antivirus software on servers

- and desktops, and keep it updated.
- Consider blocking or quarantining some content at the email server.
- Educate users about the proper handling of attachments received over the network.

the people who don't know security would find it difficult to use."

But that approach leaves too many holes, warned consultants. And blocking features such as ActiveX is not an option for many firms. "In the e-commerce age, it is no longer a valid solution to block technologies," said Nimrod Vered, director of product management for Finjan Software. "This can lead to a loss of competitive advantage."

Increasingly, companies are also realising that antivirus software, both on the desktop and the server, is not enough. "The CA InnoculateIT antivirus software [that we use] detected but couldn't cure I Love You," said Paul Alan, business information manager for Marshall Aerospace in Cambridge.

Nick Galea, director of GFI, which has a product called Mail Essential for Exchange/

SMTP that can intercept scripts and viruses, said, "The problem with antivirus software is that you can only block things that you know about. It is nice, but it's only a very small part of the security puzzle."

Modern viruses and worms, such as Love Letter and Melissa, move too quickly for traditional antivirus approaches, Galea said. Firms will increasingly need something like an email firewall, even for messages going out, and to quarantine every script and macro unless it is absolutely essential.

Galea said a more worrying threat is worms that work quietly and target specific firms – something antivirus vendors will not be able to easily detect.

▼ [Love Letter hurts Microsoft, p26](#)
 ▼ [Antivirus flaws, p67](#) ▼ www.microsoft.com/technet/security/tools.asp