*Should organisations really jettison Microsoft's flagship web server software, ISS?*

# Microsoft unplugged

**WHO USES WHAT?**

*Microsoft's IIS – Internet Information Services – is a module of Windows 2000 Server and the Personal Web Sharing systems that come with Windows 98 and other client operating systems. The Netcraft research web site, which automatically monitors the number of Internet sites in operation and the server software they use, reports that, of the web servers using SSL (Secure Sockets Layer) security, over half use IIS. However, of all web servers, IIS represents 25% of the total, with the open source package Apache taking the lead at 50%.*

It was a bombshell that hit Microsoft's Internet product strategy out of the blue. In September 2001, the world's largest technology analyst group, Gartner, recommended that organisations put future purchases of Microsoft's IIS (Internet Information Services) web server software on hold. They also advised users to remove existing copies and replace them with alternative products.

This radical advice was based on the fact that several computer viruses and worms, including the notorious Code Red and Nimda worms, had exposed multiple security holes in IIS — weaknesses that Microsoft has been slow to fix. A blunt statement from Gartner analyst John Pescatore followed: "Recent viruses have shown the high risk of using IIS," he said. His words have prompted frantic activity among systems administrators, who are applying security patches to copies of IIS on an almost-weekly basis.

## DIFFICULT DECISIONS

But the advice to ditch IIS in favour of alternatives, such as Sun Microsystem's iPlanet web server or the open source Apache code, raises troublesome questions: Is a switch of web server a practical proposition for most organisations and are rival products any more secure?


Some organisations seem to have already answered those questions with a resounding 'yes'. Netcraft, a web service that tracks application and web server usage across Internet sites worldwide, reports that, since July 2001, 80,000 addresses that previously used IIS have been taken down. Of these, 2,000 have restarted using a different web server.

On a much more worrying scale, a poll of web administrators by US-based industry newspaper *Internet Week* in October revealed that around 40% had already removed IIS. Only 19% said they had no intention of ditching it.

But moving to an alternative server software may not be a practical proposition for many companies, according to some consultants. Rob Enderle at the Giga Information Group cautions that the cost of switching to a completely new web server will prove very high, even though some products are free or have a low licence overhead. "Typically, the server is highly integrated with the rest of the operation, including databases and publishing systems. If you remove the web server, you have to extract and replace its links to these systems," says Enderle.

"A knee-jerk response isn't the right strategy," agrees Frank Prince of Forrester Research. "In any case, other vendors don't have bug-free products."

## TOO CUMBERSOME

Microsoft points to certain security vulnerabilities in Apache to show that IIS is not alone in facing security problems (although, to date, far fewer flaws have been uncovered in Apache). Additionally, Apache is typically used to power 'vanilla' web server activity, while IIS is often involved in ecommerce, according to Netcraft.

Nevertheless, Microsoft concedes that it has made it hard for customers to maintain a secure system. "As a customer, it's very difficult to get secure in the first place, and then it's very difficult to ensure that you continue to stay secure as new threats or vulnerabilities come to light," says Brian Valentine, senior vice president of Microsoft's Windows division. "Our current system [of updates] is too cumbersome, too time-consuming, too hard. We need to increase our engineering investment and work to minimise vulnerabilities."

In response — and to discourage customers from migrating to other platforms — Microsoft has devised a Strategic Technology Protection Programme to help users secure their sites, and it has also released software tools to 'lock down' servers in the event of a security exposure.

But Gartner's Pescatore thinks this is too little, too late. He claims IIS will not be a secure product until Microsoft has rewritten it completely and put the software through the sort of public testing programme that Apache has undergone.

Ultimately, Enderle and Prince both maintain that the problem is not actually one with IIS *per se*; rather, it is induced by a combination of Microsoft's position as a 'highly visibility' target for hackers and a lack of emphasis on security at many organisations.

For large organisations with a significant IIS investment, abandoning Microsoft IIS is hardly a realistic option. But Microsoft will need to find concrete ways to stop the Gartner message triggering a staged retreat from the product.

CONTACT
Rob Buckley rbuckley@infoconomy.com