Essential fortification checklist

By Michael Cobb

- Try out the many free tools available from Microsoft before deciding which additional security products your IIS server needs.
- Subscribe to the newsgroups and forums that cover any products you purchase in order to stay up-to-date.
- Don't install any of the samples and examples that come with a new product on your production server.
- Secure your most important resources first, and check that your choice of product does indeed protect them.
- Develop a Network Service Access Policy to define the features that your firewall must have.
- Deploy an intrusion-detection system to provide security against imperfect products, and new and old vulnerabilities. Monitoring your system will help you catch a hacker regardless of what vulnerability they exploit to gain access.
- Log files are only useful if you read them. Get a log analyzer, or a product that includes one, to automate the auditing and analysis of your network logs.
- Choose an antivirus tool that centralizes control and can interact with other security products.
- Implement Change Control and Back-Up Policies, and supplement them with restoration software to recover from Web defacements.
- Get senior management on board as part of your security awareness training program to educate your staff about the need for security and their security-related duties.
- Stress test your Web site to see if it can handle peak loads, and consider adding SSL-accelerator hardware if you're running an e-commerce site.
- Decide whether you need strong authentication for those clients or users that need access to very sensitive information on your server, and issue them security tokens.
- Find holes before hackers do by using a vulnerability scanner.

- Download the CIS Scoring Tool, and check if your IIS configuration matches industry best practice.

- If you don't have enough qualified security staff in-house, consider outsourcing some duties such as site monitoring.

- Keep your documentation up to date. Use a network documentor if you're managing a big enterprise network.