October 2, 2001

Microsoft Security: Securing Internet Information Server

Michael Rasmussen

Catalyst

Recent news

Question

My organization has made a commitment to Internet Information Server (IIS), and it does not make sense to get rid of it as some recommend. What can we do to secure IIS?

Answer

Many organizations have made a significant investment in IIS, and find its features and integration capabilities of tremendous business benefit. This makes a recommendation to move to another platform costly and infeasible.

What many fail to realize is there are steps that can be taken to significantly improve the security in IIS. Giga provides the following recommendations:

1. **Harden** — All systems should be adequately "hardened" before production deployment. Hardening is the process of securing a system through configuration. Standard hardening steps can be found in Planning Assumption, Security Maintenance — Essential Components in Security Architectures, Michael Rasmussen. Operating systems and applications, especially **Microsoft**'s, do not default to what is considered a secure installation and require configuration and tuning. Checklists and documents of Microsoft-recommended hardening practices for Windows and IIS can be found on the Microsoft Web site.
2. **Maintain** — Vulnerabilities in products are discovered continually, with Microsoft products under the microscope of hackers more than anyone. As a result, organizations that want secure systems must maintain security regularly through security configurations review and application of patches.
3. **Enhance** — Security in Microsoft products can be enhanced through other products. Some tools to enforce security are available free from Microsoft, such as; IISLock, which turns off unneeded features in IIS; URLScan, which protects IIS servers from many forms of attacks; and HFNetChk, which checks for missing patches. Other products, such as **Entercept**'s Web Server Edition, **Sanctum**'s AppShield, and eEye SecureIIS offer commercial products that enhance IIS security.
4. **Monitor** — Systems, especially those connected to the Internet, need to be monitored for security incidents. The use of intrusion detection systems augments this process. Organizations using intrusion detection systems during recent attacks, such as Nimda, have found they were able to respond quickly and minimize the impact on their environment. At a minimum, logs should be reviewed on a regular basis.
5. **Pressure** — Microsoft, as with any vendor, needs to understand that security is important to its clients. Clients should provide regular feedback to vendors about security in their products, and hold them accountable when the vendor ignores security.