

Patch Management

Update your server with the latest security patches and service packs

The Proactive Approach

Proactive security risk management has many advantages over a reactive approach. Instead of waiting for bad things to happen and then responding to them afterwards, you minimize the possibility of the bad things ever occurring in the first place. You make plans to protect your important assets by implementing controls that reduce the risk of vulnerabilities being exploited by malicious software or attackers.

The Patch Management Process

Patch management is a circular process and must be ongoing. The unfortunate reality about software vulnerabilities is that, after you apply a patch today, a new vulnerability must be addressed tomorrow.

Develop a patch management process that includes each of the following:

DETECT. Use tools to scan your systems for missing security patches. Try MBSA (Microsoft Baseline Security Analyzer) <http://www.microsoft.com/technet/security/tools/mbsahome.mspix> or Red Hat Network http://www.redhat.com/en_us/USA/rhn/.

ASSESS. If necessary updates are not installed, determine the severity of the issue(s) addressed by the patch and the mitigating factors that may influence your decision.

ACQUIRE. If the vulnerability is not addressed by the security measures already in place, download the patch for testing.

TEST. Install the patch on a test system to verify the ramifications of the update against your current configuration.

DEPLOY. Deploy the patch to your server. Make sure your applications are not affected. Employ your rollback or backup restore plan if needed.

MAINTAIN. Subscribe to notifications that alert you to vulnerabilities as they are reported – good ones you might want to consider are Microsoft Security Notification Service (alerts can be received through MSN, Windows Messenger, e-mail or mobile device) or Sans (both Linux and Windows and other platforms). Then begin the patch management process again.

Identifying Patch Requirements

As an ongoing process, you need to ensure that your server patches are up to date. In some cases, a new patch will be released that you will need to install on all your servers. You should continue to analyze all of your servers to ensure that they are completely up to date with all of the latest patches. To efficiently keep your servers up to date, you need to know what vulnerabilities exist and what protection is already in place.