Keep Hackers Out of Your Content

By Bill Wong

January, 2001

Keeping a Web site up to date is a major chore and there are some people that like to change your content when no one is looking. Lockstep's WebAgain 2.0 does not prevent unauthorized changes from occurring but it does fix them quickly. It also reports any tampering to the site so that preventative measures can be improved.

WebAgain is a service that runs on Windows NT or Windows 2000. It keeps track of up to five Web sites on different servers by comparing the contents a copy of a Web site's contents with that on the other servers. It does this on a regular basis. Web site servers can run on any operating system including Windows. Unauthorized changes are noted and the WebAgain administrator is notified. The changes are then removed and typically quarantined. Finally, the original contents of the Web site are restored.

These steps are what any web administrator would do to keep a Web site accurate. The only difference is that WebAgain does it 24x7 and it does not miss minor visual differences because the files and directory comparisons are binary.

WebAgain is not only useful in its ability to keep a Web site intact but can also be setup to mimic the Web site and FrontPage Server Extension support. This is combined with WebAgain's ability to update its managed Web sites when any changes occur to its local copy. The FrontPage Server Extension support allows these changes to be made using Microsoft FrontPage or a compatible editor.

WebAgain works equally as well with Web site editor and management tools that do not utilize FrontPage Server Extension support. This includes applications like Netscape Composer and Macromedia Dreamweaver. The documentation provides step-by-step instructions for using these kind of applications with WebAgain.

WebAgain's version control system keeps track of prior versions including updates made via the FrontPage Server Extension. Version control is also a fast way to backup a known web site configuration should the CEO decide that the new home page looks like garbage.

Lockstep understands the importance of backups and the version control system is just one part of the solution. The WebAgain Rescue Kit is the other. The Rescue Kit is a basic backup for a set point in time that can be saved on removable media. It provides finer grain control than a tape backup of the WebAgain directories that include the complete contents of the version control system database.

WebAgain can operate using a modem connection in addition to a dedicated connection. The on-demand modem support will be important for smaller sites hosted on an ISP's site. It is easy to setup a schedule and WebAgain retries if there is a problem connecting to the Internet.

WebAgain servers can be administered remotely. This is handy on LANs where the administrator has a PC that is not the WebAgain server. Likewise, remote access over the Internet is possible but WebAgain does not provide any tunneling support. Instead, reliable and secure LAN access must be provided through other means such as a VPN gateway. Remote administration is controlled by a password and it can also be limited to a set of IP addresses.

We had no trouble setting up and using WebAgain. Our server was setup on Windows NT Server. The test sites were an ISP hosted site with FTP access and some Internet Information Servers (IIS) running on LAN PCs. The initial configuration was easy since the ISP hosted site was already setup. It was a simple matter to configure the FTP support and download the first configuration into WebAgain's version control system.

The next step was to setup the LAN sites using WebAgain. This was simply a matter of adding the sites to the check list and then updating them from the current version of the web site. We also setup the schedule for checking all these sites. Each site is configured independently so WebAgain can take advantage of high-speed links to some sites and low speed links to other sites.

Checking can also be fine tuned. Important folders, such as the location of the home page, can be scanned more frequently than the whole site. There is also Fast and Regular scan methods. Fast compares file sizes and time stamps. Regular compares contents and takes longer. A typical configuration we tried checks the home folder often using the

Regular scan, the entire site using the Fast scan every couple hours, and a complete Regular scan daily.

WebAgain's checking also locates files that have been added. Extra files are often a symptom or precursor to turning the web server into a zombie server. Zombie servers are proxies in denial-of-service attacks. The extra files are often triggers or applications that invoke these attacks. Extra files can also be referenced by web pages providing data like unauthorized graphics in a corrupted web page.

We also tried the various notification and logging methods. Email and SNMP (Simple Network Management Protocol) can be used to note changes to monitored sites. POP3 Email notification supports a list of email addresses and SNMP requires a third party SNMP management system. SNMP support is typically used in larger organizations that utilize SNMP for general network monitoring. Logging utilizes the Windows Event Log. Each feature can be enabled or disabled.

WebAgain required minimal regular maintenance. The size of the version control database may be of concern if the site is large and the WebAgain server is storage limited. Otherwise, the only work we did with WebAgain was when we corrupted the test sites and received notification of the changes. We had to check the quarantined files.

WebAgain did a great job of keeping a web site up to date and made distributing site changes to multiple sites easier. It caught all the changes we made including adding files that were not part of the original site but it does not help in finding out who is making changes. Tracking down an attacker takes significantly different techniques than WebAgain can apply and, especially with remote ISP sites, may require monitoring access that is normally inaccessible to web site managers. Still, WebAgain is invaluable at noticing attacks, determining when and what occurred and correctly problems before they cause significant problems.

WebAgain is a bargain for medium to large sites especially multiple server sites but it can be a bit expensive for small web sites. Of course, even in the latter case, the price of corruption can easily exceed the price of WebAgain. If it fits in the budget, we heartily recommend WebAgain.

Company Details:
Lockstep Systems Inc.
P.O. Box 1906
Scottsdale, AZ 85252-1906
www.lockstep.com

Product Details:
$995 for up to 5 Web sites

Contact:
Karl Forster
480-596-9432
kforster@lockstep.com

William Wong is a network consultant and author. He has been the Director of PC Magazine's PC Labs and is currently a Technology Editor for Electronic Design. His latest book is Windows 2000 DNS from Osborne/McGraw-Hill.