## Operational Issues

Another critical area to monitor is your daily operating procedures.

### Environmental Hazards

If you don't already have sensors checking the traditional HVAC concerns—heat, ventilation, and air conditioning—in your server rooms, install them. While you're doing that, don't forget about the possibility of water leaks, flaking plaster, or loose wires. The best monitoring tool is the human eyeball, either peering through a remote camera or peeking through a doorway. Set up a weekly or monthly schedule for inspections, or install a minicam in the more remote locations to bring key images to your desktop.

### Physical Access

Installing security software does no good if someone can walk in and carry off the equipment—or just bang it with a sledgehammer. It's not uncommon for the server room to share space with the computer lab or for the wiring closet to

## Monitoring Technologies

We've compiled a list of tools to help you deal with the various areas of monitoring, along with recommendations on how often to use them. The products named here are examples only and are not necessarily endorsed by the authors. Although not included here, multifunction hardware technology from such companies as 3Com, ServGate, SonicWall, and Symantec may also provide effective security solutions.

| | OBJECTIVE | SAMPLE TOOLS | FREQUENCY |
|---|---|---|---|
| Vulnerability Scanning | Identify technical weaknesses in software, hardware, and system configurations. Some scanning tools include integrated patch management, registry repair, and software update utilities. | **Web servers:**<br>Achilles (www.mavensecurity.com)<br>N-Stealth (www.nstalker.com)<br>SpikeProxy (www.immunitysec.com)<br>**Network:**<br>Microsoft Baseline Security Analyzer (www.microsoft.com/technet)<br>Nessus (www.nessus.org)<br>NetIQ Security Analyzer 5.1 (www.netiq.com)<br>Shavlik EnterpriseInspector (www.shavlik.com)<br>Sun Microsystems SunSolve (sunsolve.sun.com)<br>Symantec Vulnerability Assessment (enterprisesecurity.symantec.com) | Web servers should be checked when there are vulnerability advisories and significant Web site changes are made. Total network scans should take place at least twice a year. Firewall and e-mail servers should be scanned daily to weekly. |
| Network Traffic Analysis | Monitor bandwidth usage to verify network performance; identify traffic patterns; and provide forensic evidence of intrusions and inappropriate network use. | CyberGauge (www.neon.com)<br>Iris Network Traffic Analyzer (www.eeye.com)<br>ntop (www.ntop.org)<br>Snort (www.snort.org) | Monthly; daily, if problems are suspected |
| Password Testing | Verify that user passwords are appropriate and effective. | Cain & Abel (www.oxid.it/cain.html)<br>John the Ripper (www.openwall.com/john)<br>LophtCrack (www.crack.cd/l.1.html) | Same as number of days between password changes |
| Intrusion Detection | Test the effectiveness of firewalls. | dsniff (www.monkey.org/~dugsong/dsniff)<br>Norton Personal Firewall (www.symantec.com/sabu/nis/npf_mac)<br>Snort (www.snort.org) | Daily |
| Wireless Network Detection | Detects unauthorized wireless access points. | AirSnort (airsnort.shmoo.com)<br>Kismet (www.kismetwireless.net) | Yearly or whenever system changes are made |
| Virus Detection and Content Filtering | Detect and eliminate viruses, worms, Trojan horses, and other malicious software; detect and reduce spam; and limit access to undesirable Web sites. | Network Associates (www.nai.com/us)<br>Sophos AntiVirus (www.sophos.com)<br>Symantec Antivirus (enterprisesecurity.symantec.com)<br>SurfControl (www.surfcontrol.com) | Daily |
| Network Threat Information | Stay informed of current threats. | Internet Security Systems Alert Center (gtoc.iss.net/issEn/delivery/gtoc/index.jsp)<br>SANS InternetStormCenter (isc.sans.org)<br>Symantec DeepSight Threat Management System (enterprisesecurity.symantec.com) | Daily |
| Data Integrity Checking | Verify whether data files have become corrupted and detect installation of unauthorized software. | Tripwire (www.tripwire.com) | Monthly |
| Network Logs | To remain informed of network and server activities. | Backup logs<br>Server, firewall event, and virus detection logs | Daily |