Five ways to simplify the vulnerability management lifecycle

Scott Sidel, CISSP, CEH, ETC
May 2005
Why do we patch?

- **No system is perfect.**
  - Vulnerabilities ship “out-of-the-box”

- **Threats “on the wire”**

- **Even while a system is being built it is a target.**
  - The need for a “Build” VLAN
What gets patched?

- OS
- Applications
- Network Appliances
What gets patched?

- **OS**
  - Out of the box, operating systems must be brought up to date
  - Even Unix and Linux must be patched
    - Up-To-Date [Red Hat]
    - `apt-get` (Advanced Packaging Tool) [Debian]
    - YUM (Yellow-dog Updater Modified) [Fedora]
  - Rolling in *NIX updates during the build
    - Jump Start [Solaris]
    - Kick Start [Linux]
What gets patched?

- **OS**
  - **Windows**
    - Windows Update
    - Windows Software Update Services (SUS)
    - Windows Update Services* (WUS)
    - System Management Server (SMS)
What gets patched?

- Applications
  - A patching method for every application?
    - Office Update
    - Adobe Updater
    - Real Audio / Windows Media Player
    - Norton Live Update
    - AdAware Reference Files
    - Firefox Software Update
What gets patched?

- **Appliances**
  - Cisco Routers
    - 11.3AA
  - Check Point Firewalls
    - NG FP3 HF2
  - Juniper NetScreen Firewall
    - R3
  - McAfee IDS/IPS
    - 2.1
How do I know there is a patch?

- Vendor Alerts
- Vulnerability Alert Lists
  - SearchSecurity
    - www.searchsecurity.com
  - US-CERT
    - www.us-cert.gov
  - CERT
    - www.cert.org
  - SANS
    - www.sans.org
  - Insecure
    - www.insecure.org
  - BugTraq
    - www.securityfocus.com
- Visit the sites
- Sign up for the mailing lists
- Subscribe to RSS news feeds
When do I patch?

- Whenever I get around to it?
- Ad-Hoc
  - As patches come out
- After Hours
- Maintenance Window
  - Third Tuesday of Every Month at 2 AM
- Microsoft’s “Patch Tuesday”
Do I know what to patch?

- **Vulnerability Scanning**
  - Find vulnerabilities
  - Follow-up to validate that vulnerabilities were patched
    - “(Don’t) Trust but verify”

- **CVE**
  - Common Vulnerabilities and Exposure list
    - Standardized names for vulnerabilities
  - [www.cve.mitre.org](http://www.cve.mitre.org)
Can you afford to patch?

- (Hours x Rate x Systems) = Cost to Patch

- If you have four techs ($80 billing rate/hour) patching 300 systems, one hour per system, you would spend $96,000.

- If you have four techs ($80 billing rate/hour) patching 1000 systems, one hour per system, you would spend $320,000.
Can you afford not to patch?

- **Elements of loss:**
  - Lost productivity
  - Loss of revenue
  - Intellectual property losses
  - Loss of assets
  - Legal/regulatory costs
  - Embarrassment (do not underestimate)

- Now the labor looks like a better value.
What to look for

- Platform (or cross-platform) Coverage
  - Windows
  - Solaris
  - Linux

- Ease of Deployment
  - What good is a system that never gets used?
What to look for (cont.)

- **Multi-Site Rollout**
  - Different divisions
  - Different geographic locations

- **Patch Rollout Control**
  - Flood or throttle
  - Retries, load on next boot, load on next connect (mobile users)

- **Rollback**
  - Ability to remove patches if it breaks something
What to look for (cont.)

- **Validation**
  - Verify patch with multiple scanners
  - Isolate noncompliant devices
  - Schedule remediation for off-peak times

- **Reporting**
  - Technical
  - Management
Five Ways to Simplify Vulnerability Management
Five final points on patching

1. **Establish Repeatable Processes**
   - Don’t let every patch be a fire drill
   - Create patching policies and guidelines
   - Know when to patch; assess patches
   - Establishing testing and release processes
   - Create communication channels to staff
   - Set SLAs/cooperative agreements with business departments
Five final points on patching

2. Maintain Accurate Inventory
   - Operating Systems
   - Applications
   - Network Devices
   - Locations
   - Connection Types
   - Assign Values to Devices/Resources/Assets
Five final points on patching

3. Assign Roles and Duties to Staff
   - Admins should have pre-assigned devices, applications or machines to patch
   - Train staff to react when patches are released and made available for deployment
   - Establish goals and standards for patch management (time to deploy, quality testing)
   - Monitor staff’s work
Five final points on patching

4. **Verify, Verify, Verify**
   - Don’t trust your patch management system
   - Use multiple scanners to verify patch deployments
   - Practice 80/20 rule until you reduce the number of unpatched machines
   - Use endpoint security solution/quarantine zones to isolate noncompliant systems
Five final points on patching

5. Start Over

- Establish metrics to measure effectiveness of patching
  - Time to patch vs. SLAs
  - Number of machines patch/time
- Identify soft spots, make adjustments
- Update asset and valuation inventory
- Training staff on changes
Questions

- What is the meaning of life?