Patch Management Best Practices

NETBankAudit works with customers on a daily basis on ways to improve the complex patch management environments. Below is a list of procedures and software that can help in this ever changing business need.

Patch Management Best Practices

- All installed software and versions should be documented with business need.
  - Questions to ask here are what is the business need for Adobe Air and Flash.
  - Oracle Java version requirements should be documented.
  - If outdated software is required for business operations it should be formally documented in a risk assessment including a statement from the vendor.
    - A plan should be developed with the vendor to ensure future software is compatible with the latest and most secure plugins.
- All installed software is part of the patch management program.
- All workstations and servers should be part of the patch management program.
- The patch management program has to have an automated tool to deploy and manage the patching process. This tool or tools should address both Microsoft and 3rd party patching.
- Prior to deployment a procedure to roll back the patch should be verified.
- Patches should be deployed to test groups that cover a sample of all workstation environments. Once the patches are deployed to the test group all production applications should be tested for errors.
- Once testing confirms no adverse impact to the patch they should be installed on all equipment in a phased approach.
- Ensure users do not have the ability to disable/stop patches from installing. Patch after hours, use a GPO to remove the shutdown button, etc.
- **The patching process needs to be actively managed by IT staff.** Regular review by staff on the status of deployed patches and investigating and correcting failed patch installs.
  - This process should also include verification that out of date applications are uninstalled. For example, some versions of Oracle Java will not uninstall previous versions.

Tools to Assist with Patch Deployment/Management

- BMC IT Asset Management Software - http://www.bmc.com/it-solutions/asset-management.html
- Dell Kace Endpoint Systems Management and Deployment – http://software.dell.com/kace/
- Flexera Corporate Software Inspector - http://www.flexerasoftware.com/enterprise/products/software-vulnerability-management/corporate-software-inspector/
- GFI LanGuard - http://www.gfi.com
- Kaseya VSA – http://www.kaseya.com/products/vsa
- LAN Desk Patch Manager - http://www.landesk.com/products/patch-manager/
- Lumension Endpoint Management and Security Suite – https://www.lumension.com/vulnerability-management/patch-management-software.aspx
- MS Windows Server Update Service (WSUS) - http://technet.microsoft.com/en-us/wsus/default.aspx
- Shavlik Patch – http://www.shavlik.com/products/patch/
- Solar Winds Patch Management – http://www.solarwinds.com/patch-manager.aspx
- Symantec Client Management Suite powered by Altiris technology – http://www.symantec.com/client-management-suite/