OVERCOMING PATCH MANAGEMENT PITFALLS

Brad Ruppert, CISSP
GIAC G7799, GIAC GSLC
Objective

- Identify Importance of Patch Management
- Run through Patch Management Lifecycle
- Examine Patch Management Approaches
- Identify Patch Management Roles/Responsibilities
- Discuss Common Pitfalls
- Provide Solutions to Common Patching Issues
- Outline Steps to Successful Patch Management
Importance of Patch Management

- Mitigate Vulnerabilities
- Protect Assets
- Provide Stability
- Reduce Risk
- Reduce Liability
- Reduce Downtime
- Protect Reputation
Approaches to Patch Management

- Top Down
  - Management mandates it through policy so administrators need to comply

- Bottom Up
  - Administrators push the issue to increase stability and protect systems they are responsible for

- Blended
  - Management and administrators are equally determined to implement a successful patch management strategy
The Process

- Assess
  - Assets, Vulnerabilities, Infrastructure, Resources
- Identify
  - Required Patches, Updates, Criticality, Roles
- Evaluate and Plan
  - Responsibility, Resources, Timelines, Testing
- Deploy
  - Schedule Downtime, Coordinate Groups, Push out Patches, Host Follow-up Meeting
Common Pitfalls

- Failure to obtain executive support
- Getting caught up in the low level details
- Failure to go through change control
- Failure to have a rollback plan
- Failure to adhere to patching timelines
- Failure to identify dependencies between systems
- Failure to communicate or involve all necessary groups
Overcoming Pitfalls

- Utilize ISSC meetings to gather executive support
- Form Patch Management Committee
- Establish S.M.A.R.T milestones
- Spend time with system administrators to gather requirements and feedback
- Document the entire process including roles, responsibilities, timelines, testing, system dependencies
<table>
<thead>
<tr>
<th>Role</th>
<th>Responsibility</th>
<th>Job Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>Patching Administrator</td>
<td>Acquire/Deploy Patches</td>
<td>System Admin</td>
</tr>
<tr>
<td>System Support</td>
<td>Bring systems back online</td>
<td>Configuration Mgmt. Engineer</td>
</tr>
<tr>
<td>Application Support</td>
<td>Bring application back online</td>
<td>Application Engineer</td>
</tr>
<tr>
<td>Quality Assurance</td>
<td>Run smoke tests</td>
<td>QA Engineer</td>
</tr>
<tr>
<td>System Monitor</td>
<td>Verify systems are back online</td>
<td>Network Ops Engineer</td>
</tr>
<tr>
<td>Patching Auditor</td>
<td>Run compliance reports</td>
<td>Information Security Analyst</td>
</tr>
<tr>
<td>Business Approval</td>
<td>Provide sign off</td>
<td>Change Control</td>
</tr>
</tbody>
</table>
Starting approach

- Identify assets that need patching
- Work with system administrators to develop achievable patching window
- Work with ISSC and change control to solidify monthly/quarterly patching cycle
- Develop Patch Management Procedure
- Develop Patch Management Committee
- Have the committee certify the procedure
Things to watch out for:

- Be wary of the “Blame Game”
- Having your patching window trumped by other projects/managers
- Weakness in communication between I.T. groups during patching window
- Burning out your system administrators, QA, or application support groups
Ensuring Success

- Document a detailed patching-window timeline incorporating each step needed for complete recovery
- Work with small groups when coordinating details to prevent getting sidetracked
- Have a valid reporting structure and audit regularly
- Communication is key (system announcements, bridge line, committee meetings, change control meetings)
Ensuring Success (2)

- Host follow-up meetings with committee members and patching support groups
- Track open issues or problems that occurred during patching and assign action items
- Provide praise to those that did a great job
- Budget for rewards (movie tickets, lunch vouchers, gift cards) to those that deserve it
Effective Patch Management can help protect against system compromise, data breach, or even unplanned system downtime. Assigning ownership and responsibility is key. Enterprise Patch Management requires excessive communication to multiple groups across the business and I.T. Successful Patch Management can be one of the most cost effective solutions in helping securing the enterprise, but should not be treated as a “Silver Bullet”.
Success is not final, failure is not fatal: it is the courage to continue that counts.

- Winston Churchill