Patch Management Checklist

This patch management checklist outlines the steps and procedures that an organization should follow in order to effectively manage and deploy software patches. It is designed to help you avoid common mistakes, simplify patch management policy and increase cybersecurity.

Patch Management Strategy Preparation

- [ ] Create a patch management policy
- [ ] Create or test backups of all your critical systems
- [ ] Create a good roll-back plan to reverse the patches if something goes wrong quickly
- [ ] Set up patch management software to implement updates

Pre-Deployment Research

- [ ] Inventory all your assets
- [ ] Define or update the scope of patch management, e.g., identify which assets need to be patched
- [ ] Split the endpoints into groups based on operation system type. For example, the test environment of Windows servers, the test environment of Linux servers, the production environment of Windows servers, etc.
- [ ] Split the systems into groups based on application update
- [ ] Split the systems into groups based on SLA (low, medium, and high availability)
- [ ] Identify all software, information, objects, databases, and hardware in the System that require updates
- [ ] Identify the core stakeholders for each system
- [ ] Identify maintenance days for each system
- [ ] Identify systems downtime for each asset
- [ ] Identify exceptions
- [ ] Obtain formal approval from the system stakeholder for patching and system downtime before starting the update process
- [ ] Gain temporary remote access to the target system to perform its update

Procuring Patches

- [ ] Upload necessary patches to your patch management system
- [ ] Set the patch management system as a network proxy hub for your patches

Pre-Deployment Patch Testing

- [ ] Create a test environment that will contain all types of systems in your scope
- [ ] Deploy relevant patches to the test environment on the scheduled date and time
- [ ] Check that the test system works as intended
- [ ] If problems are found, record them in detail, along with how critical they are. The security team and the system owner analyze this information, assess the risk, determine whether to install the update in the production environment, and record the decision and reasoning.
- [ ] The system owner reviews and approves the results of the updates tested in the test environment and grants permission to implement the updates in the production environment

Patch Implementation

- [ ] Provide advance notice of at least 24 hours for any planned system unavailability resulting from upgrades.
- [ ] On the scheduled maintenance day, implement updates on the designated systems or system group in accordance with their service level agreement, beginning with systems that have the lowest SLA.
- [ ] Deploy updates to the system in the production environment.
- [ ] Verify the system's proper functioning. If any issues are identified, the system owner evaluates the severity of the problem and, if necessary, grants approval for rolling back the update.
- [ ] Record the successful patch deployment results

Post Implementation Process

- [ ] Ensure that the technical documentation for the system is updated after each update is completed.
- [ ] Conduct a monthly check for new updates, with a special focus on Patch Tuesday.
- [ ] Perform monthly vulnerability scans to identify new security vulnerabilities
- [ ] Audit checklist regularly depending on the process change