National Campaign
for
Cyber Hygiene
Count, Configure, Control, Patch, Repeat

TOOLKIT
for
PATCH

National Campaign for Cyber Hygiene

Count, Configure, Control, Patch, Repeat

Introduction

In this digital age, we rely on our computers and devices for so many aspects of our lives that the need to be proactive and vigilant to protect against cyber threats has never been greater. However, in order to be as secure as possible, we need to **use good cyber hygiene** - that is, making sure we are protecting and maintaining systems and devices appropriately and using cyber security best practices.

The Campaign, a joint effort of the Center for Internet Security (CIS) and the Governors Homeland Security Advisors Council (GHSAC), aims to create a nationwide movement toward measurable–and sustainable–improvements in cybersecurity.

The Cyber Hygiene Campaign is a multi-year effort that provides key recommendations for a low-cost program that any organization can adopt to achieve immediate and effective defenses against cyber attacks.

The Campaign has developed toolkits for each of its key recommendations to provide easily understood instruction sheets and information for entities to improve their cybersecurity posture. The toolkits are: Count, Configure, Control, Patch and Repeat. These toolkits are dynamic documents and will continue to evolve to meet the ever-changing cyber threat landscape. In addition, a unique Executive Measurement Guide will be issued to assist Executives in the implementation of the toolkits.

For more information about the Cyber Hygiene Campaign, and to access electronic versions of the toolkits, please visit the Campaign website at: http://www.cisecurity.org/about/CyberCampaign2014.cfm

Join the cause and show your commitment to getting cyber healthy by signing the online pledge! Take the Cyber Hygiene Pledge: www.cisecurity.org/cyber-pledge

Special thanks to the following individuals who were instrumental in the development of the toolkits:

- Jonathan Trull, Chief Information Security Officer
  Qualys, Inc.
- Deborah A. Snyder, Acting Chief Information Security Officer
  NY State Office of Information Technology Services
- Gary Coverdale, Assistant CIO/CISO
  Information Technology Services, Napa County, California
- Members of the Cyber Hygiene Panel

Center for Internet Security®

Governors Homeland Security Advisors Council

National Campaign for Cyber Hygiene

Count, Configure, Control, Patch, Repeat

Table of Contents

National Campaign for Cyber Hygiene

Count, Configure, Control, Patch, Repeat

I. Plain English Guide for Patch

Basic Questions to Better Cyber Security Hygiene

Cyber Hygiene Priority -- PATCH: Protecting your systems by keeping current!

Patch and vulnerability management is a security practice designed to proactively prevent the exploitation of IT vulnerabilities that exist within an organization. The expected result is to reduce the time and money spent dealing with vulnerabilities and exploitation of those vulnerabilities. Proactively managing vulnerabilities of systems will reduce or eliminate the potential for exploitation and involve considerably less time and effort than responding after an exploitation has occurred. (NIST Special Publication 800-40 Version 2.0)

1. Why is this step important?

Properly applied patch processes will allow for:

- appropriate patching that fix 'bugs' and vulnerabilities identified in third party software
- addressing security flaws in code, software and applications that your organization relies upon on a daily basis
- an extra layer of security since your environment is being scanned constantly to expose and exploit vulnerabilities; this is especially true of content management systems for websites
- timely patching of security issues, which is critical to maintaining the operational availability, confidentiality and integrity of (IT) systems
- reduced risk to operating systems and application software, which is one of the most common security issue identified by security and IT professionals

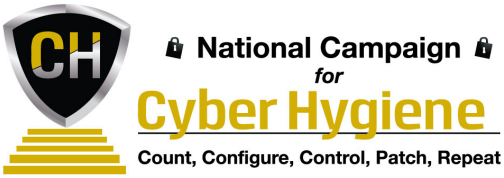
2. What to do?

Review your organization's technology asset inventory and identify what software is operating on these assets (software inventory). Your inventory should include:

- Operating systems
- PC applications
- Server based applications and OSs
- Web applications
- Content management systems
- Mobile Applications
- Printer/Scanner operating software
- Switches / configurations

Continually review what patches, updates, and revisions need to be applied and then, after appropriate testing, apply them in a timely and systematic process. Types of patches include:

- Microsoft security Updates
- MS-ISAC and CIS vulnerability notifications
- Vendor notifications and postings
- Security and privacy blogs
- Fixes from your own testing of internally developed applications



3. Who should be responsible to do this?

No two organizations are exactly alike. Some have CIOs, others CISOs, still others have CTOs, and some even have EIEIOs. Whoever in your organization has responsibility for installing and maintaining your IT equipment and systems should have the lead for conducting the inventory of your IT assets and for maintaining a process to ensure the count stays accurate. If you don't have an a person in charge of IT, identify someone who is organized and responsible to do the inventory.

An assigned team should be fully responsible for your patching process, however you will need to have support from your business centers (departments, supported agencies, etc.) to fully test specific patches on applications prior to deploying patches.

Pick a specific day of the week and make that your standard "patch day", say, for instance "Patch Wednesday". There are many reasons why "patch day" should be standardized:

- All staff will get used to that particular day when they will expect their PC to be updated.
- The following day, trouble shooters can first look at applied patches if they get help desk calls the morning following the patching process (usually patches will not break systems, but there may be impacts in some cases.

4. When to do it?

Deploy your routine patches the same day and time every week or month. That way staff can anticipate those periods and provide a higher alert if a patch impacts operability. Your Help Desk staff can also associate problems happening with patch timing to look at those areas first when troubleshooting technology problems.

At least monthly, technology administrators should review resources that discuss patches and updates in those areas that your organization has applications running. Multi-State Information Sharing and Analysis Center (MS-ISAC) is a great resource for vulnerability analysis and reporting that will help you stay ahead of the process.

5. Where to start?

- Utilize your organization's Inventory of IT resources (hardware and software) to determine which hardware equipment, operating systems, and software applications are used within the organization. Keep this as a snapshot of what your organization looks like in regard to focal points of hardware and software patching, updating, and versioning. Make sure your "patching team" is notified when new equipment or software are deployed in your organization. Review your organization's inventory monthly to ensure you capture new add-ons to your technology environment in your patching process.
- Monitor security sources for vulnerability announcements, patch and non-patch remediations and emerging threats that correspond to the software within the systems inventory.
- Review your 3rd party application vendors and user groups to review patches and updates that are being published.
- Prioritize the order in which the organization addresses remediating vulnerabilities.
- Create a database of remediations that need to be applied to the organization.
- Conduct testing of patches and non-patch remediations on IT devices that use standardized configurations.
- Assign responsibility to oversee vulnerability remediation.
- Distribute vulnerability and remediation information to local administrators.

- Perform automated deployment of patches to IT devices using enterprise patch management tools.
- Configure automatic update of applications whenever possible and appropriate.
- Verify vulnerability remediation through network and host vulnerability scanning.
- Train administrators on how to apply vulnerability remediations.
- Identify and document any exceptions to the patching process with an explanation as to why the patching cannot be conducted (e.g. custom application that is not compatible with update).

A proper patch management process takes time, however it is time well spent, because if done improperly, it can bring systems down for hours if not days.

6. How to do it?

- Implement specialized automated patching software that will push out to specific systems updates to operating systems, enterprise and specific applications to your asset hardware (PCs, servers, printers, scanners, etc.).
- Get support for testing software patches before they are deployed by having responsible departmental 'power users' that can help pre-test the affects of software application patches.
- Utilize tools like Microsoft's Baseline Security Analyzer (MBSA), a free download that scans PCs and servers on a network for configuration anomalies and missing security patches.
- You can sign up for the Microsoft Security Bulletin, which is published a week before patch day and provides information about the nature of the vulnerabilities to be patched, the affected software. As part of patching process, Microsoft releases patches monthly and categorizes them as either "critical" or "important."
- Test the patches in a lab or pre-production environment to determine if they might cause an outage on production servers. A test lab should mirror your production servers as closely as possible, and should be used to check that functionality isn't affected after a patch is installed. (At the most basic level, make sure that servers reboot after patch installation). Testing is easier if you've already established a baseline configuration for your servers; for example, documenting how they should be configured.
- Make sure you have a 'back-out' process that can quickly reverse the patch or update that negatively impacts your systems. Remember that you will not be able to fully insure compatibility during a testing process so having a back-out plan is critical to providing continued access to technology resources.

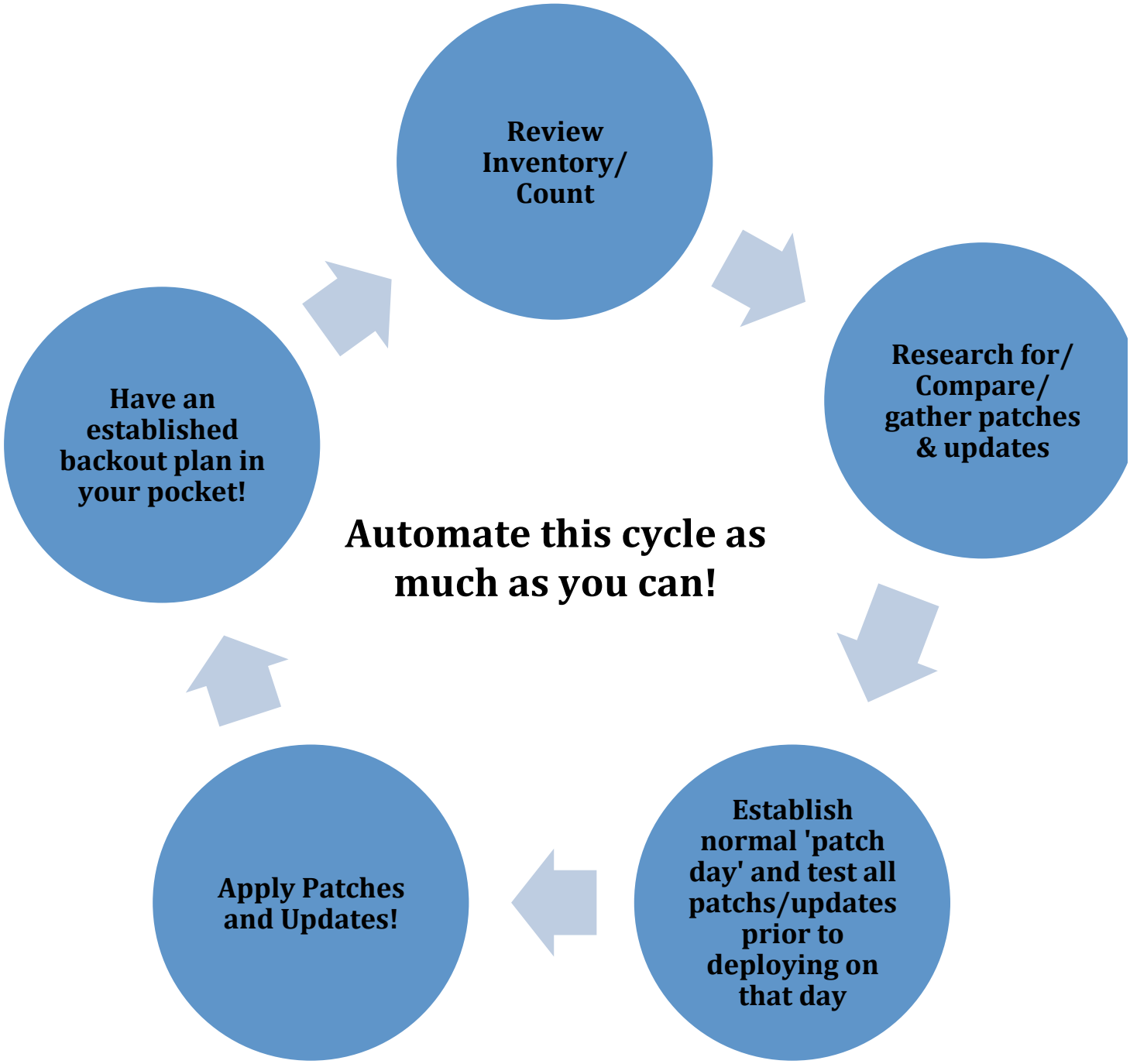
IT staff can test patches on their own PCs. While this is adequate for basic testing, don't forget to test patches on a variety of devices, including notebooks. **Conduct this testing in different departments because operating systems and software will vary** and the impact of a patch can only be fully assessed if distributed to a wide sample of users.

A comprehensive testing procedure will involve more than just installing a patch and making sure a system still boots. Scripts can be run on servers to perform a series of tests that confirm vital functionality hasn't been affected by the update. PowerShell or VBscripts can run through the tests automatically to accelerate the process and generate reports. For instance, which Windows services should run in your baseline configuration? After a patch is installed and the server rebooted, are all of the required services still running?

National Campaign for Cyber Hygiene

Count, Configure, Control, Patch, Repeat

The Patch Cycle



National Campaign for Cyber Hygiene
Count, Configure, Control, Patch, Repeat

II. Technical How-To Guide for Patch

Tasks to consider

Tasks Included in level	**LOE (Level of Effort - resources, effort ,cost)** High Med, Low	**Priority** How important is it for implementation of security program/controls (High Med, Low)	**Completion Criteria**
Review your Technology Asset Inventory (all hardware, servers, software, mobile devices) • Check for patch updates, • Test • Deploy • Automate • Backout	High	High	You have defined resources and have a benchmark of what is patched and what is not.
Develop a methodology to test all systems prior to apply patches, updates, and fixes.	Med	High	Automate testing tools and processes implemented to insure patches will not impact your systems.
Deploy an automated tools and develop scripts that push out patches	Low	Med	Patches are automatically dispersed.
Validate that patches are being deployed	Med	Med	Patches are validated and after each deployment to ensure consistent remediation

Resources:
For ideas on conducting an IT asset inventory see the following links:

Resources	**Link**
SANS Institute InfoSec Reading Room Patch Management	http://www.sans.org/reading-room/whitepapers/iso17799/patch-management-2064
Essentials of Patch Management Policy and Practices	http://www.patchmanagement.org/pmessentials.asp
SANS Institute InfoSec Reading Room: A Practical Methodology for Implementing a	http://www.sans.org/reading-room/whitepapers/bestprac/practical-methodology-implementing-

National Campaign for Cyber Hygiene
Count, Configure, Control, Patch, Repeat

Resources	Link
Patch management Process	patch-management-process-1206
Microsoft Best Practices	http://technet.microsoft.com/en-us/library/cc750077.aspx#XSLTsection124121120120
SANS Global Information Assurance Certification Paper- Patch Management Best Practices	http://www.giac.org/paper/gsec/2999/patch-management-practices/105015

III. How to Measure Guide for Patch

There are a couple of different measurements that can be of use for you to track how effective your patch management program is. This is by no extent a full list of metrics possible, but a simply something that you may want to consider given the information you may or may not have at hand.

Contemplate keeping track of the percentage of your assets which are missing at least one critical patch. This metric will rely on leverage your asset inventory and your monitoring of patch deployment

The score could be derived from the following equation:

(# _of_devices_with_missing_critical_patches)/ (total_number_of_devices)*100

You can also modify this equation with additional information that you may be collecting such as the criticality of the assets that are patched and unpatched. Additionally, depending on which patch solution you are using, many of these have robust means to generate reports on the progress and comprehensiveness of the patches. Research and utilize these features to form the foundation of your metrics tracking.

National Campaign for Cyber Hygiene
Count, Configure, Control, Patch, Repeat

IV. Additional Resources for Patch

The Cyber Hygiene Toolkits are dynamic documents and will continue to evolve to meet the changing cyber threat landscape. In addition, a unique Executive Measurement Guide will be issued to assist Executives in the implementation of the toolkits.

For more information about the Cyber Hygiene Campaign, and to access electronic versions of the toolkits, please visit the Campaign website at: http://www.cisecurity.org/about/CyberCampaign2014.cfm

If you have expertise, resources or information relating to any of the following areas that you could share for subsequent editions of the toolkits, **please contact us at 518.880.0699 or contact@cisecurity.org**:

- Case Studies
- Webcasts, Podcasts, Videos [e.g., YouTube]
- Mentor Programs [to pair experienced individuals with those looking to gain more expertise]
- Upcoming Events [trainings, conferences, roundtable discussions]
- Other

Youtube channel	**Link**
Podcasts	
Windows Server Update Services (24min)	http://www.youtube.com/watch?v=f4_UoxXJ9Cg
WSUS- IT Free Training (54min)	http://www.youtube.com/watch?v=E1dOJpBJAHU

V. Mapping to NIST Cybersecurity Framework

"Patch" maps to the following NIST Framework function(s) and Subcategories:

NIST Framework Function	**Subcategory(s) / Description(s)**
Identify. Risk Assessment	ID.RA-1: Asset vulnerabilities are identified and documented
Identify Patches and Updates	ID.RA-2: Threat and vulnerability information is received from information sharing forums and sources
Protect. Information Protection, Processes and Procedures	PR.IP-12: A vulnerability management plan is developed and implemented