CRITICAL CYBERSECURITY HYGIENE: PATCHING THE ENTERPRISE

The National Cybersecurity Center of Excellence (NCCoE) is addressing the challenge of improving enterprise patching practices for general information technology (IT) systems through collaborative efforts with industry and the IT community, including vendors of cybersecurity solutions. This fact sheet provides an overview of the Critical Cybersecurity Hygiene: Patching the Enterprise project, including challenge, proposed solution, and potential benefits. If you have questions or suggestions, please contact us at cyberhygiene@nist.gov.

CHALLENGE

There are a few root causes for many data breaches, malware infections, and other security incidents. Implementing a few relatively simple security hygiene practices can address those root causes—preventing many incidents from occurring and lowering the potential impact of incidents that still occur. In other words, security hygiene practices make it harder for attackers to succeed and reduce the damage they can cause.

Unfortunately, security hygiene is easier said than done. IT professionals have known for decades that patching software—operating systems and applications—eliminates vulnerabilities. Despite widespread recognition that patching is effective, it's also resource-intensive. And the act of patching can reduce system and service availability, but delaying patch deployment gives attackers a larger window of opportunity.

Patching is a particularly important component of cyber hygiene, but existing tools are insufficient for many situations. For example, many organizations lack tools to help them measure and assess the effectiveness and timeliness of their patching efforts. Many organizations also struggle to prioritize patches, test patches before deployment, and adhere to policies for how quickly patches are applied in different situations.

PROPOSED SOLUTION

Building on previous National Institute of Standards and Technology (NIST) work documented in *NIST Special Publication (SP) 800-40 Revision 3, Guide to Enterprise Patch Management Technologies*, and *NIST SP 800-184, Guide for Cybersecurity Event Recovery*, the NCCoE and its collaborators are developing a proposed approach to improve enterprise patching practices for general IT systems. We are using commercial and open source tools to aid with the most challenging aspects, including system characterization and prioritization, patch testing, and patch implementation tracking and verification. We will include actionable, prescriptive guidance on establishing policies and processes for the entire patching lifecycle, to include defining roles and responsibilities for all affected personnel and establishing a playbook containing mitigation actions for destructive malware outbreaks.

BENEFITS

The NCCoE's practice guide to Patching the Enterprise can help organizations:

- increase their awareness of the importance of security hygiene
- understand what actions they can take in the short term to overcome common obstacles involving enterprise patching for general IT systems
- learn how they can achieve a comprehensive security hygiene program based on existing standards, guidance, and publications
- improve their recovery from incidents that occur and minimize the impact of incidents on the organization and its constituents

The National Cybersecurity Center of Excellence (NCCoE), a part of the National Institute of Standards and Technology (NIST), is a collaborative hub where industry organizations, government agencies, and academic institutions work together to address businesses' most pressing cybersecurity challenges. Through this collaboration, the NCCoE develops modular, easily adaptable example cybersecurity solutions demonstrating how to apply standards and best practices using commercially available technology.

LEARN MORE ABOUT NCCOE
Visit https://www.nccoe.nist.gov

CONTACT US
nccoe@nist.gov
301-975-0200

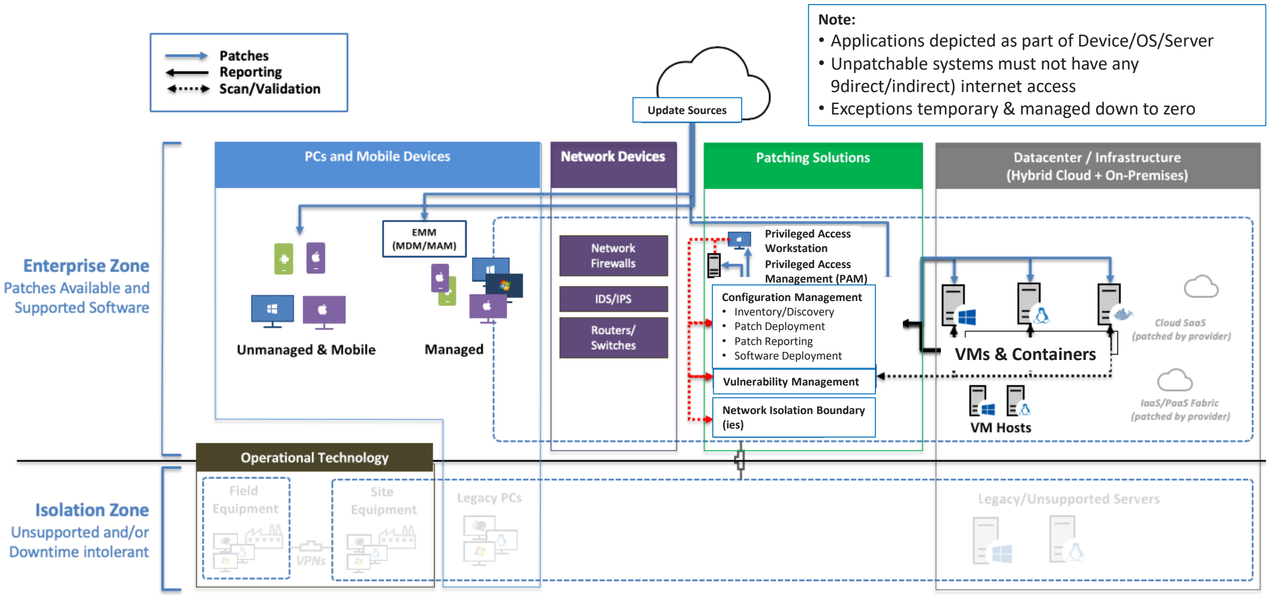
HIGH-LEVEL ARCHITECTURE

The proposed solution is focused on common enterprise services in the IT environment. Patching system components include:

- Configuration management tools (where patching is usually managed)
- Vulnerability assessment to provide independent assessment of whether updates are applied correctly
- Security components for the patching and configuration management infrastructure
- Network isolation boundaries that protect systems from attacks on eternally unpatched vulnerabilities (unsupported, sensitive to operational downtime, etc.)

The high-level architecture will also include these components:

- Managed PCs, unmanaged PCs, and mobile devices, along with their apps, firmware (for the PCs only), and an Enterprise Mobility Management (EMM) solution for managing the mobile devices
- Network devices, including firewalls, intrusion detection systems/intrusion prevention systems, routers/switches, and network-based storage systems
- External update sources controlled and managed by third parties
- Datacenter/infrastructure (hybrid of cloud and on-premises) including virtual machines (VMs) and containers, VM hosts, and apps



Note:
- Applications depicted as part of Device/OS/Server
- Unpatchable systems must not have any 9direct/indirect) internet access
- Exceptions temporary & managed down to zero

TECHNOLOGY COLLABORATORS

The technology vendors participating in this project submitted their capabilities in response to an open call in the Federal Register. Companies with relevant security capabilities were invited to sign a Cooperative Research and Development Agreement with the National Institute of Standards and Technology (NIST), allowing them to participate in a consortium to build this example solution. Technology collaborators on this project are...

CISCO eclypsium FORESCOUT FOXGUARD SOLUTIONS

Microsoft SALTSTACK tenable

Certain commercial entities, equipment, products, or materials may be identified by name or company logo or other insignia to acknowledge their participation in this collaboration or to describe an experimental procedure or concept adequately. Such identification is not intended to imply special status or relationship with NIST or recommendation or endorsement by NIST or the NCCoE; neither is it intended to imply that the entities, equipment, products, or materials are necessarily the best available for the purpose.

DOWNLOAD PROJECT DESCRIPTION

This fact sheet provides a high-level overview of the work underway on enterprise patch management. For more details, download the project description by visiting https://www.nccoe.nist.gov/projects/building-blocks/patching-enterprise or scan the QR code which takes you to the Patching the Enterprise project page.

HOW TO PARTICIPATE

As a private-public partnership, we are always seeking insights from businesses, the public, and technology vendors. If you have questions about this project or are interested in contributing technology or expertise, please send an email to cyberhygiene@nist.gov.

February 2020