Patch Management Policy

Overview

Passwords are an essential component of computer security. They are the first line of defense for user accounts. An improperly designed password might compromise the entire corporate network of COMPANY-NAME.

As a result, all COMPANY-NAME employees or volunteers/directors (including contractors and suppliers having access to COMPANY-NAME systems) are responsible for selecting and securing their passwords, as detailed below.

Read More: Patch Management Policy - A Practical Guide

Purpose

Computing systems and applications contain security flaws. These weaknesses enable the development and spread of malicious software, interrupting typical corporate activities and putting COMPANY-NAME in danger.

To prevent this risk, software "patches" are made available to remove a specific security vulnerability.

Given the number of computer workstations and servers on the COMPANY-NAME network, a robust patch management solution that can successfully deploy security patches when they become available is required.

Adequate security requires the participation and support of every COMPANY-NAME employee and the Board of Directors.

This policy intends to provide direction, create goals, enforce governance, and outline compliance.

Audience

This policy is applicable to every employee, contractor, consultant, temporary staff, and the Board of Directors of COMPANY-NAME. It covers all equipment, whether owned or leased by

COMPANY-NAME, including electronic devices, servers, software applications, computers, peripherals, routers, and switches.

Policy Detail

Many computer operating systems, such as Microsoft Windows, Linux, and others, include software application programs that may contain security flaws.

Occasionally, one of those flaws permits a hacker to compromise a computer. A compromised computer threatens the integrity of the COMPANY-NAME network and all computers connected to it. Almost all operating systems and software applications have periodic security patches released by the vendor that need to be applied.

Patches that are security-related or critical should be installed as soon as possible.

In the event that it cannot centrally deploy a critical or security-related patch, it must be installed in a timely manner using the best resources available.

Failure to properly configure new workstations is a violation of this policy. Disabling, circumventing, or tampering with patch management protections and/or software constitutes a policy violation.

Responsability

The Head of IT is responsible for providing a secure network environment for COMPANY-NAME. COMPANY-NAME's policy is to ensure all computer devices (including servers, desktops, printers, etc.) connected to COMPANY-NAME's network have the most recent operating system, security, and application patches installed.

Every user, individually and within the organization, is responsible for ensuring prudent and accountable use of computing and network resources.

IT is responsible for ensuring all known and reasonable defenses are in place to reduce network vulnerabilities while keeping the network operating.

IT Management and Administrators are responsible for monitoring security mailing lists, reviewing vendor notifications and Web sites, and researching specific public Web sites for the release of new patches.

Monitoring will include, but not be limited to:

- Scheduled third-party scanning of COMPANY-NAME 's network to identify known vulnerabilities;
- Identifying and communicating identified vulnerabilities and/or security breaches to {COMPANY-NAME} 's VP of IT;
- Monitoring Computer Emergency Readiness Team (CERT), notifications, and Web sites of all vendors with hardware or software operating on COMPANY-NAME 's network.

The IT Security and System Administrators are responsible for maintaining the accuracy of patching procedures, which detail the what, where, when, and how to eliminate confusion, establish routine, provide guidance, and enable practices to be auditable.

Documenting the implementation details provides the specifics of the patching process, which includes specific systems or groups of systems and the timeframes associated with patching.

Once alerted to a new patch, IT Administrators will download and review it. The patch will be categorized by criticality to assess the impact and determine the installation schedule.

Patching Guidelines

1. Patch Testing

For critical assets, the IT Department might choose to evaluate the patch in a controlled environment to identify potential business interruptions or other concerns. Patches not passing this assessment might be omitted from the patching routine, provided the IT Department adheres to the Exception and Mitigation procedures.

If everything seems fine, you can proceed with deploying your patches throughout your system. However, remember that even if patch providers conduct tests, those tests might not perfectly align with your specific environment. So, ensure you also validate them in your own context.

2. Patch Deployment

It's important to recognize that not every patch will install flawlessly. Sometimes, a patch could incapacitate a device or inadvertently disrupt other IT systems or applications. With this

in mind, the IT Department should always implement the Disaster Recovery Policy before initiating the Patch Management process.

At a minimum:

- Ensure that a comprehensive system backup is executed before applying any update.
- Conduct a thorough data backup prior to the update.
- For crucial systems like routers, servers, etc., undergoing firmware updates, a standby system might be necessary in case the primary device malfunctions due to the update.
- Should any update fail, the IT Department will strive to revert the system or software to its former version to regain its functionality. In cases where a rollback isn't possible, the system must either be restored from backup or replaced immediately.

3. Automated Patch Management

Numerous vendors provide automated patching options for their specific software. Moreover, various third-party tools and service agencies are available to help with the patch management procedure.

Where feasible, the IT Department should leverage suitable methods to streamline the patching process. Such automated systems can lighten the workload of the IT Department and ensure timely patch updates across the IT landscape. Before initiating any automated solutions, the IT Department should verify that all patch management preparations are in place.

It's recognized that certain firmware, IT devices like routers, and software providers might necessitate manual updates. Those offering automated patching services should clearly state what they can and cannot patch or update, and the asset inventory should indicate which items need manual attention.

4. Patch Verification and Testing

After the patching and updating is finalized, the IT Department must ensure that the patches were successfully implemented. If not, they should document and rectify any issues. They should also confirm that the vulnerabilities targeted by the patches have indeed been addressed.

Any persisting vulnerabilities need to be dealt with accordingly:
- **Failed Patches**: Updates that didn't install as intended.
- **Disruptive Patches**: Updates that, when installed, might result in significant business interference.
- **Unneeded Patches**: Updates not related to security that introduce or rectify features that are unnecessary or undesired.
- **Unpatched Vulnerability**: Certain assets may still possess vulnerabilities which remain unpatched due to various reasons such as the product reaching its end of life, the vendor no longer operating, and so on.

5. Audit and Compliance

Executives and auditors from COMPANY-NAME can request records and proof of patch management processes when needed. The documentation and evidence might comprise:

- Authorized Maintenance Timeframe Requests
- Sanctioned Exclusion Lists
- Logs of updates and patches for primary system and utility groups
- These logs should list system ID, patching date, status of the patch, any exceptions, and the reasons for such exceptions
- Evident infrastructure that upholds company-wide patch management for systems, software, and equipment
- Reports on Patch Management.

Enforcement

Employees who intentionally violate this policy may face disciplinary measures, including possible termination. The performance evaluations of IT Department staff entrusted with this policy's implementation will partially or wholly depend on their adherence to its expectations.

Consistent failure by the IT Department to uphold the standards of this Patch Management policy may be viewed as negligence, leading to potential disciplinary measures. Providing false reports or demonstrating extreme negligence might lead to immediate termination or other disciplinary actions.

This policy presumes that organizations unable to meet the update standards due to resource constraints will not blame their IT Department when faced with excessive workload or

pressure. Organizations with unrealistic expectations may witness frequent staff changes within the IT Department and challenges in keeping skilled and proficient personnel.

Distribution

This policy should be provided to all executives of COMPANY-NAME as well as IT Department staff who oversee and manage the Patch Management Policy.

Anyone involved in patch management tasks or impacted by this policy, especially executives and potentially other pertinent staff, should be given a copy. Those in charge of implementation might be required to formally confirm that they have received it.

Policy Version

Version 1.0

Date of Approval:

Overview:

Endorsements

Endorsed By: _____
[Patch Management Authority Endorsement]

Endorsed By: _____
[CEO or Relevant Executive]

An endorsement from the Patch Management Authority confirms agreement with the policy's requirements and signifies a commitment to uphold them. An endorsement by the CEO or a related executive implies the policy aligns with the organization's objectives. The executive endorsing should hold a position of sufficient authority to ensure adherence to the policy across various departments.