Overview

Passwords are an important aspect of computer security. They are the front line of protection for user accounts. A poorly chosen password may result in the compromise of {COMPANY-NAME}'s entire corporate network. As such, all {COMPANY-NAME} employees or volunteers/directors (including contractors and vendors with access to {COMPANY-NAME} systems) are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

Read More: Vulnerability Patch Management As A Service

Purpose

Security vulnerabilities are inherent in computing systems and applications. These flaws allow the development and propagation of malicious software, which can disrupt normal business operations, in addition to placing {COMPANY-NAME} at risk. In order to effectively mitigate this risk, software "patches" are made available to remove a given security vulnerability.

Given the number of computer workstations and servers that comprise the {COMPANY-NAME} network, it is necessary to utilize a comprehensive patch management solution that can effectively distribute security patches when they are made available. Effective security is a team effort involving the participation and support of every {COMPANY-NAME} employee and the Board of Directors.

This policy is to assist in providing direction, establishing goals, enforcing governance, and to outline compliance.

Audience

This policy applies to all employees, contractors, consultants, temporaries, and the Board of Directors at {COMPANY-NAME}. This policy applies to all equipment that is owned or leased by {COMPANY-NAME}, such as, all electronic devices, servers, application software, computers, peripherals, routers, and switches.

Adherence to this policy is mandatory.

Policy Detail

Many computer operating systems, such as Microsoft Windows, Linux, and others, include software application programs which 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 many software applications have periodic security patches, released by the vendor, that need to be applied.

Patches, which are security related or critical in nature, should be installed as soon as possible.

- In the event that a critical or security related patch cannot be centrally deployed by IT, 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 violation of policy.

Responsibility

The VP of IT is responsible for providing a secure network environment for {COMPANY-NAME}. It is {COMPANY-NAME}'s policy 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, both individually and within the organization, is responsible for ensuring prudent and responsible 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 that have hardware or software operating on {COMPANY-NAME}'s network

The IT Security and System Administrators are responsible for maintaining 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 the new patch. The patch will be categorized by criticality to assess the impact and determine the installation schedule.