RESOURCE INF-009G

Patch Management Guideline

Purpose

This guideline provides direction with regard to managing patches that are used to protect Coast Mountain College's (CMTN's)computer systems and applications.

Overview

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 CMTN at risk. 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 CMTN network, it is necessary to use 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 CMTN employee and the Board of Directors.

Definitions

Computer Emergency Readiness Team (CERT): A group of information security experts responsible for the protection against, detection of, and response to an organization's cybersecurity incidents.

Scope

This guideline applies to all employees, contractors, consultants, temporaries, and the Board of Directors at CMTN. This guideline also applies to all equipment that is owned or leased by CMTN, such as, all electronic devices, servers, application software, computers, peripherals, routers, and switches.

Adherence to this guideline is mandatory.

Details

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 CMTN 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 guideline. Disabling, circumventing, or tampering with patch management protections and/or software constitutes a violation of the guideline.

Responsibility

The VP of IT is responsible for providing a secure network environment for CMTN. CMTN ensures that all computer devices (including servers, desktops, printers, etc.) connected to CMTN'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 CMTN's network to identify known vulnerabilities
- identifying and communicating identified vulnerabilities and/or security breaches to CMTN's VP of IT
- monitoring Computer Emergency Readiness Team (CERT), notifications, and web sites of all vendors that have hardware or software operating on CMTN'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 the new patch. The patch will be categorized by criticality to assess the impact and determine the installation schedule.

Related Policies, Guidelines, and Other Resources

- None