Standard: Patching and Malicious Code Management

Contents

Revision History

Standard	Effective Date	Email	Version	Contact	Phone
OIT-PMCMS		strevena@csustan.edu	1.0	Stan Trevena	209.667.3137

Executive Summary

Stanislaus State is highly diversified in the information that it collects and maintains on its community members. It is the university's responsibility to be a good steward and custodian of the information that it has been entrusted, which must be upheld by all members of the university. Patch and Malicious code management is an important part in reducing and mitigating threats and vulnerabilities. Patching and Malicious Code Management standard defines the requirements for applying patching and malicious code execution security controls for machines under the control of Stanislaus State. The threat landscape is evolving toward attacks targeted against vulnerable client software or targeted attacks against users with previously unknown vulnerabilities against endpoint workstations. These standards of due care will help manage the risk of loss of confidentiality, integrity, and availability of Stanislaus State's sensitive information.

Introduction and Purpose

This standard defines the requirements for applying patching and malicious code execution security controls for machines under the control of Stanislaus State. The threat landscape is evolving toward attacks targeted against vulnerable client software, or targeted attacks against users with previously unknown vulnerabilities against endpoint workstations. These standards of due care will help manage the risk of loss of confidentiality, integrity, and availability of Stanislaus State's sensitive information.

Scope

This standard applies to all Stanislaus State, Self-Fund, and Auxiliary ("campus") computer systems and facilities, with a target audience of Stanislaus State Office of Information Technology (OIT) employees and partners.

Standard

This standard establishes and documents Patching and Malicious Code Management requirements based on Stanislaus State business requirements. This standard is reviewed annually by the Information Security Officer and updated as new security controls evolve to mitigate the threat of malicious code execution.

Patching Controls

All machines on the campus, regardless of Operating System or virtualization, must implement a patching application that will help improve the security posture on campus endpoints wherever supported. The application shall have the ability to remotely apply third party and operating system patches to endpoints. If the Operating System is not supported by the patching application, departments are responsible for manually applying and documenting application of all relevant security patches.

Approved Patching Application

Endpoint workstations will use an approved patching application that should be configured to query the central server in order to learn the required patches. This application service should not be tampered with or disabled by users. Users are prohibited from running other patching applications.

Patching Updates Applied at Scheduled Intervals

The patching application will be configured to download and install required operating system and 3rd party patches at the scheduled intervals. Patches shall be applied and the machine shall be restarted at least once every 31 days. Required patches include but are not limited to Operating System, Adobe Suite, Acrobat, Apache, Flash, Java, Office, Oracle, SQL Server and ALL 3rd party applications for which security patches are available.

Supported Operating Systems

Endpoints connected to the campus wired or Wi-Fi networks are required to run a currently supported operating system which receives regular security evaluations and updates. Any exceptions must be approved and documented by the Information Security Officer.

Preventing Malicious Code Execution

The campus will implement, through the Information Security Officer, controls that will help to detect, prevent, and recover against malicious code. In addition, user awareness procedures should be implemented, in accordance with the user "Information Security Awareness Training" standard [2].

Systems Network Access Requirements

Systems without the required software patches or systems that are virus-infected must be disconnected from the Stanislaus State network, or placed in a quarantine/isolated VLAN for containment.

Eradicating Computer Viruses

Any user who suspects infection by a computer virus, worm, spyware or some other malware, must immediately shut-down the involved computer, disconnect from all networks, call the OIT Help Desk, and make no attempt to eradicate the involved software.

Virus Eradication by Systems Administrators

Users must not attempt to eradicate a computer virus from their system unless they do so while in communication with an OIT Technician/System Administrator.

Downloading External Software

Workers must not knowingly download untested, unknown, or malicious software.

Software Scanning

Workers must not use any externally-provided software from a person or organization other than a known and trusted supplier unless the software has been scanned for malicious code and approved by the Information Security Officer or a local information security coordinator.

Virus Test System

Whenever software or files are received from any external entity, this material must be tested for viruses, worms, and other malicious software on a stand-alone non-production machine before it is used on Stanislaus State information systems.

Outbound Software and Executables

All files containing software or executable statements must be certified as virus free prior to being sent to any third party.

Virus Disclaimer for Downloaded Files

Stanislaus State uses industry-standard virus protection software on its computer systems, and regularly updates this software. In spite of these and other controls that Stanislaus State maintains, it is possible although unlikely that files downloaded from our web site may contain a computer virus. Every user downloading files from Stanislaus State is therefore strongly advised to scan the files with their own virus protection software before opening or executing these same files. Stanislaus State is not responsible for any damage or disruption that files downloaded from its web site or commerce site may cause. Anti-Virus Software Installation Virus screening software must be installed and enabled on all Stanislaus State servers, desktops and laptops. This includes Microsoft operating systems, OS X, and Linux operating systems as well as managed and unmanaged (off campus) endpoints. Protective measures will also be deployed on the Stanislaus State at the firewall (Data Center and Border) to screen/analyze/quarantine malicious software.

Anti-Virus Software Installation

Virus screening software must be installed and enabled on all Stanislaus State servers, desktops and laptops. This includes Microsoft operating systems, OS X, and Linux operating systems as well as managed and unmanaged (off campus) endpoints. For more information on Stanislaus State Antivirus visit https://www.csustan.edu/blackboard/plugins-readers-software [3].

Scanning Downloaded Software

Before software downloaded from non-Stanislaus State sources is decompressed, it must be screened with an approved virus detection package after the user has logged off from all servers and terminated all other network connections.

System Integrity Checking

All Stanislaus State personal computers and servers must run, at the very least on a daily basis, integrity checking software that detects changes in configuration files, system software files, application software files, and other system resources.

Virus-Checking Programs

Virus checking programs approved by the Information Security Officer must be continuously enabled on all local area network servers and networked computers regardless of operating system. All State/Self-Fund/Auxiliary owned machines are required to report into a central management console. Any exceptions shall be approved and documented by the Information Security Officer.

Decrypting Files for Virus Checking

Where applicable, all externally-supplied computer-readable files must be decrypted prior to being subjected to an approved virus checking process.

Software Write Protection

Where operationally feasible and aside from when it is being installed, reconfigured, or when it must modify itself in order to properly execute, all software running on personal computers and workstations must be write-protected such that an error will be generated if a computer virus or malware attempts to modify the software or operating system. In general, users shall not login to workstations or servers with administrative credentials; administrative credentials shall be reserved for temporary elevation of privilege for administrative tasks. Local administrative access to user computers will be disabled by default, but 24-hour admin access can be requested via the Help Desk when software needs to be installed by the user that writes to the Windows Registry.

Scanning Backup Files for Viruses

Where operationally feasible, before any files are restored to a production Stanislaus State computer system from backup storage media, these files must have been scanned with the latest version of virus screening software.

Involvement with Computer Viruses

Users must not intentionally write, generate, compile, copy, collect, propagate, execute, or attempt to introduce any computer code designed to self-replicate, damage, or otherwise hinder the performance of any Stanislaus State computer or network.

Portable Computers Issued with Standard Configuration

Stanislaus State issued portable computers must be configured according to standards issued by the Office of Information Technology (OIT), portable computer configurations must include access controls which prevent users from changing the configuration or installing software. All computers procured by any means shall first be configured by an appropriate OIT technician prior to usage. All portable computers must be configured to utilize the firewall remote software for protection against malicious software.

Downloading Internet Mirror Site Software

Software resident on Internet mirror sites must not be downloaded to any Stanislaus State computer unless it is received directly from a known and trusted source and software verification tools like digital signatures are employed.

Downloaded Information

All software and files downloaded from non-Stanislaus State sources through the Internet or any other public network must be screened with virus detection software prior to the software being executed or the files being examined through another program.

Approvals for Software Usage and Licensing

Regardless of value, before end-users utilize new software or web applications to provide or store Stanislaus State data, they must first obtain approval of the involved software license agreement from the department manager (MPP) and follow purchasing guidelines set by the Procurement department. Before providing this approval, the department manager must fully understand the functionality of the software, what data is being stored in the software, determine that it is fully compliant with Stanislaus State's Information Security Requirements, and receive written approval from the Data Owner prior to usage.

Regular Monitoring of Public Web Site for Malicious Software

System Administrators must annually perform a search of all public-facing internet computers for possible infection of malicious software.

Preventing Mobile Code Execution

Where the use of mobile code is authorized, the configuration should ensure that the authorized mobile code operates according to a clearly defined security standard, and unauthorized mobile code should be prevented from executing.

Review of Accounts Used in Applications and Middleware

Stanislaus State managers (MPP's) must annually review and approve the privileges of special accounts used to access production content, applications or middleware.

More Information

[1] Stanislaus State: "Stanislaus State Patching Controls"

[2] Stanislaus State: "Information Security Awareness Training"

[3] Stanislaus State: "Stanislaus State Antivirus"