SILICON VALLEY CLEAN ENERGY

ITP8

Category: INFORMATION TECHNOLOGY

MALWARE DEFENSE POLICY

I. PURPOSE

The purpose of this policy is to prevent data loss, corruption, or misuse of SVCE computing resources or information that may occur when malware is introduced to SVCE's IT network.

II. SCOPE

This policy applies to all SVCE personnel and to all computer hardware and software comprising SVCE's IT network.

III. DEFINTIONS

Malware - Short for "malicious software", malware is designed to damage, disrupt, or abuse an individual computer or an entire network and/or steal or corrupt an organization's most valuable and sensitive data. Viruses, worms, and Trojan horses are examples of malware.

Spam or junk email – Unsolicited commercial email sent in bulk over the Internet. Spam puts a cost and a burden on recipients by clogging up network bandwidth, consuming disk space, and wasting employees' time. Spam is frequently a malware vector.

Subscription service – A service whereby a software vendor offers support for its product, usually for a predetermined time period. Anti-virus vendors typically include a one-year subscription (for updates, notices, etc.) with the purchase of a product license. Many vendors offer fee-based subscription services whereby subscribers automatically receive notifications, security bulletins, etc., for a set period of time.

Target – The ultimate destination for Malware; that which the malware is designed to attack. Boot sectors, hard disk drives, email servers, and departmental (HR, accounting, etc.) servers are examples of malware targets.

Vector – How malware is carried to a computer, server, or system.

Adopted: 6/14/2017
Revised: 9/13/2017

IV. POLICY

A. MALWARE DEFENSE PLANNING

How does Malware typically work and what threats exist? Malware is commonly passed to a potential Target through email. The person who receives the email opens an attachment, which unleashes the Malware, which then spreads to other computers via a shared network (Malware may attack by other means but this is a common method). To lessen the potential for damage to SVCE's Information Technology (IT) assets by Malware, the Agency should develop and implement a multifaceted approach to Malware prevention.

To prepare SVCE's Malware Defense Plan, IT Support shall review the following items:

- Threat Assessment Report
- Asset Inventory Database
- IT industry standards and best practices
- Anti-Malware vendor websites or portals
- IT security alerts and bulletins (many of which are available for free and as a subscription service).

IT Support shall use the preceding items (and possibly others) to develop a Malware Defense Plan. This Plan shall be submitted to the Chief Executive Officer for review and approval.

The Administration and Finance Department shall communicate the Plan to all employees and arrange employee training.

B. MALWARE DEFENSE PLAN

IT Support shall install firewalls on all personal computer (PC) workstations and on all servers.

IT Support shall ensure that operating systems, web browsers, email programs, and related software are configured for optimum security.

IT Support shall install an anti-virus program on every PC and server and all anti-virus software shall be automatically updated through the use of a subscription service (updates should be automatically logged by the software).

- Additional anti-malware programs should be installed on all PC's and servers to protect against nuisances such as spyware and adware, which are potential Malware Vectors.

As vendors learn of vulnerabilities (bugs) in their software and repair them, they notify registered users, post bulletins on their web sites, and notify news media that these patches are available for download. Many vendors offer

Subscription services, through which SVCE may be notified of security threats and related issues and obtain software patches.

SVCE will subscribe to one or more notification services, in order to maintain its awareness of threats and to ensure all software is updated in a timely fashion.

IT Support shall evaluate all software patches (for operating systems, browsers, email programs, applications, etc.) for relevance and criticality. If the patch is determined to be relevant (for example, an operating system security patch has more relevance - and is certainly more critical - than a foreign-language update of an application), IT Support shall install the patch in a test environment and verify its effectiveness and compatibility with existing software before installing it in the production environment. Such updates shall be logged by IT Support, if the software being patched does not automatically log activity.

All anti-malware protections shall be configured to prevent being disabled by users. Only IT Support shall be allowed to temporarily disable anti-malware measures (for example, disabling a local anti-virus program to install and configure an application locally).

SVCE shall minimize malware risks by backing up critical information.

All users shall be trained on the Malware Defense Plan at the outset. Users shall be retrained (updated) on the Plan at least once a year. The Administration and Finance Director shall be responsible for Malware Defense Plan training.

C. MALWARE DEFENSE PLAN REVIEW

IT Support shall periodically (once a week is recommended) review all anti-virus, firewall, and other relevant logs to determine if the software is up-to-date and is performing as expected. IT Support shall report its findings to the Director of Administration and Finance for possible action.

IT Support shall periodically (annually, at a minimum) meet with the Administration and Finance Director to review the Malware Defense Plan, to determine its continuing applicability and conformity to SVCE requirements.

A periodic (at least annual) audit of the Malware Defense Plan shall be conducted by an accredited auditor to determine if the Plan is in use, if it is functioning as expected, and if it conforms to standards and requirements. IT Support shall review the results of such audits, review those results with the Administration and Finance Director, and recommend changes to the Plan.

D. MALWARE DEFENSE PLAN UPDATE

IT Support shall incorporate updates into the Malware Defense Plan and ensure communication of plan changes to all employees.

Within a month of changes being made to the Malware Defense Plan, IT Support shall conduct a review with the Administration and Finance Director to verify that changes were implemented and the desired results are being achieved.

E. CONTAINMENT

Once a malware threat has been carefully analyzed it needs to be effectively contained so that the infection will not continue to

spread. IT will develop a strategy to halt malware propagation. Once the strategy has been outlined the procedures to contain the malware threat should be followed quickly and efficiently. Procedures to contain the threat may include:

a. Disable physical network access
b. Host, service, and application hardening -Vulnerable systems should be protected by applying service, application, and operating system patches as necessary
c. Power off infected systems
d. Disable network services: To shutdown network services it will likely be necessary to modify host, server, or network firewalls, and network routing devices

F. ERADICATION

After analysis and containment of a malware outbreak the threat needs to be removed from all infected hosts.

a. Scan with installed anti-malware software (make sure current definitions are installed)
b. Scan with installed antivirus software (make sure current definitions are installed)
c. Restore from backup media -use system restore, wipe drive, full format
d. Reload operating system: wipe system and load operating system

G. RECOVERY

After the malware threat has been effectively eradicated from infected hosts the process of restoring the confidentiality, integrity, and availability of system software and data begins.

a. Reinstall from installation media
b. Restore from backup media
c. Validate system state -The host should have security software reinstalled and the application software should be tested to ensure that it functions properly. It may be necessary to

restore network connectivity prior to testing application software.

d. Restore network connectivity

H. REPORT

Following successful restoration of host, network, and applications services, security administrators and management should evaluate the effectiveness of security policies and controls, and determine if any changes need to be made. It may be necessary to update the malware response plan, the acceptable use policy, corporate security plans and response measures, etc.