Overview

Malware threats must be managed to minimize the amount of downtime realized by SDCC's systems and prevent risk to critical systems and member data. This standard is established to:

- Create prudent and acceptable practices regarding anti-virus management
- Define key terms regarding malware and anti-virus protection
- Educate individuals, who utilize SDCC system resources, on the responsibilities associated with anti-virus protection

Note: The terms virus and malware, as well as anti-virus and anti-malware, may be used interchangeably.

Purpose

This standard was established to help prevent infection of SDCC computers, networks, and technology systems from malware and other malicious code. This standard is intended to help prevent damage to user applications, data, files, and hardware.

Audience

This standard applies to all computers connecting to the SDCC network for communications, file sharing, etc. This includes, but is not limited to, desktop computers, laptop computers, servers, and any PC based equipment connecting to the SDCC network.

Definitions

Read the list of common vulnerabilities here:

https://purplesec.us/common-network-vulnerabilities/

Virus: A program that attaches itself to an executable file or vulnerable application and delivers a payload that ranges from annoying to extremely destructive. A file virus executes when an infected file is accessed. A macro virus infects the executable code embedded in Microsoft Office programs that allows users to generate macros.

Trojan Horse: Destructive programs, usually viruses or worms, which are hidden in an attractive or innocent looking piece of software, such as a game or graphics program. Victims may receive a Trojan horse program by e-mail or removable media, often from another unknowing victim, or may be urged to download a file from a web site or download site.

Worm: A program that makes copies of itself elsewhere in a computing system. These copies may be created on the same computer or may be sent over networks to other computers. Some worms are security threats using networks to spread themselves against the wishes of the system owners and disrupting networks by overloading them. A worm is similar to a virus in that it makes copies of itself, but different in that it need not attach to particular files or sectors at all.

Spyware: Programs that install and gather information from a computer without permission and reports the information to the creator of the software or to one or more third parties.

Malware: Short for malicious software, a program or file that is designed to specifically damage or disrupt a system, such as a virus, worm, or a Trojan horse.

Adware: Programs that are downloaded and installed without user's consent or bound with other software to conduct commercial advertisement propaganda through pop-ups or other ways, which often lead to system slowness or exception after installing.

Keyloggers: A computer program that captures the keystrokes of a computer user and stores them. Modern keyloggers can store additional information, such as images of the user's screen. Most malicious keyloggers send this data to a third party remotely (such as via email).

Ransomware: A type of malware that prevents or limits users from accessing their system, either by locking the system's screen or by locking the users' files, unless a ransom is paid.

Server: A computer program that provides services to other computer programs in the same or other computers. A computer running a server program is frequently referred to as a server, although it may also be running other client (and server) programs.

Security Incident: In information operations, a security incident is an assessed event of attempted entry, unauthorized entry, or an information attack on an automated information system. It includes unauthorized probing and browsing; disruption or denial of service; altered or destroyed input, processing, storage, or output of information; or changes to information system hardware, firmware, or software characteristics with or without the user's knowledge, instruction, or intent.

E-mail: Abbreviation for electronic mail, which consists of messages sent over any electronic media by a communications application.

Standard Detail

All computer devices connected to the SDCC network and networked resources shall have anti-virus software installed and configured so that the virus definition files are current and are routinely and automatically updated. The anti-virus software must be actively running on these devices.

- The virus protection software must not be disabled or bypassed without IT approval.
- The settings for the virus protection software must not be altered in a manner that will reduce the effectiveness of the software.
- The automatic update frequency of the virus protection software must not be altered to reduce the frequency of updates.
- Each file server, attached to the SDCC network, must utilize SDCC IT approved virus protection software and setup to detect and clean viruses that may infect SDCC resources.
- Each e-mail gateway must utilize SDCC IT approved e-mail virus protection software.
- All files on computer devices will be scanned periodically for malware.

Every virus that is not automatically cleaned by the virus protection software constitutes a security incident and must be reported to the IT Help-Desk.

If deemed necessary to prevent propagation to other networked devices or detrimental effects to the network or data, an infected computer device may be disconnected from the SDCC network until the infection has been removed.

Users should:

- Avoid viruses by NEVER opening any files or macros attached to an e-mail from an unknown, suspicious, or untrustworthy source. Delete these attachments immediately then remove them from the Trash or Recycle Bin.
- Delete spam, chain, or other junk mail without opening or forwarding the item.
- Never download files from unknown or suspicious sources.
- Always scan removable media from an unknown or non-SDCC source (such as a CD or USB from a vendor) for viruses before using it.
- Back up critical data on a regular basis and store the data in a safe place. Critical SDCC data can be saved to network drives and are backed up on a periodic basis. Contact the SDCC IT Department for details.

Because new viruses are discovered every day, users should periodically check the Anti-Virus standard for updates. The SDCC IT Department should be contacted for updated recommendations.