Texas A&M University System Standard – Malicious Code

Standard Statement

This standard is intended to provide information to System Office information resource administrators and users to improve the resistance to, detection of, and recovery from malicious code.

Definitions

Information Resources (IR) - The procedures, equipment, and software that are designed, employed, operated, and maintained to collect, record, process, store, retrieve, display, and transmit information or data.

Malicious code - Software that is designed to operate in a manner that is inconsistent with the intentions of the user and which typically results in annoyance or damage to the user's information systems.

Examples of such software include:

- Viruses: Pieces of code that attach to host programs and propagate when an infected program is executed.
- Worms: Particular to networked computers to carry out pre-programmed attacks that jump across the network.
- Trojan Horses: Hide malicious code inside a host program that appears to do something useful.
- Attack scripts: These may be written in common languages such as Java or ActiveX to exploit weaknesses in programs; usually intended to cross network platforms.
- Ransomware: is a type of malware that infects a computer and restricts a user's access to the infected computer. This type of malware, which has now been observed for several years, attempts to extort money from victims by displaying an on-screen alert. These alerts often state that their computer has been locked or that all of their files have been encrypted, and demand that a ransom is paid to restore access.
- Spyware: Software planted on your system to capture and reveal information to someone outside your system. It can do such things as capture keystrokes while typing passwords, read and track e-mail, record the sites visited, pass along credit card numbers, and so on. It can be planted by Trojan horses or viruses, installed as part of freeware or shareware programs that are downloaded and executed, installed by an employer to track computer usage, or even planted by advertising agencies to assist in feeding you targeted ads.

Owner of an Information Resource - an entity responsible for:

- A business function; and,
- Determining controls and access to information resources supporting that business function.

Responsibilities and Standards

---

1. GENERAL

System Office (SO) information resources are strategic assets which, as property of the State of Texas, must be managed as valuable state resources. The integrity and continued operation of System Office information resources are critical to the operation of the SO. Malicious code can disrupt normal operation of System Office information resources. This standard is intended to provide information to System Office information resource administrators and users to improve the resistance to, detection of, and recovery from malicious code.

2. APPLICABILITY

This standard applies to all SO network information resources.

The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this standard are implemented. Based on risk management considerations and business functions, the resource owner may determine that it would be appropriate to exclude certain risk mitigation measures provided in this standard. All exclusions must be in accordance with standard *Exclusions from Required Risk Mitigation Measures*.

The intended audience for this standard includes all owners, managers, system administrators, and users of SO information resources.

3**.** PREVENTION AND DETECTION**:**

3.1 For each computer connected to the SO network, security updates from the manufacturer of the appropriate operating system, and/or application software, must be kept current (e.g, patched and updated).

3.2 Where feasible, individual-machine firewall software or hardware shall be installed to aid in the prevention of malicious code attacks/infections.

3.3 E-mail attachments and shared files of unknown integrity shall be scanned for malicious code before they are opened or accessed.

3.4 Diskettes and mass storage devices will be scanned for malicious code before accessing any data on the media.

3.5 Software to safeguard against malicious code (e.g., anti-virus, anti-spyware, etc.) shall be installed and functioning on susceptible information resources that have access to the SO network.

3.6 Software safeguarding information resources against malicious code shall not be disabled or bypassed.

3.7 The settings for software that protect information resources against malicious code should not be altered in a manner that will reduce the effectiveness of the software.

3.8 The automatic update frequency of software that safeguards against malicious code shall not be altered to reduce the frequency of updates.

4. RESPONSE AND RECOVERY:

4.1 All reasonable efforts shall be made to contain the effects of any system that is infected with a virus or other malicious code. This may include disconnecting systems from the network or disabling email.

4.2 If malicious code is discovered, or believed to exist, an attempt should be made to remove or quarantine the malicious code using current anti-virus or other control software. (See also standard for *Incident Management*.)

4.3 If malicious code cannot be automatically quarantined or removed by anti-virus software, the system shall be disconnected from the network to prevent further possible propagation of the malicious code or other harmful impact. The presence of the malicious code shall be reported to ITS personnel so that they may take appropriate actions in removing the malicious code and protecting other systems.

4.4 Personnel responding to the incident should have the necessary system access privileges and authority to affect the necessary measures to contain/remove the infection.

4.5 If possible, identify the source of the infection and the type of infection to prevent recurrence.

4.6 Utilize anti-virus, anti-spyware, etc. software to execute a complete system scan including the boot sector and all physical drives, to eradicate all malicious code that may be identified.

4.7 Any removable media (including diskettes, mass storage cards, etc.) recently used on an infected machine shall be scanned prior to opening and/or executing any files contained therein.

4.8 ITS personnel should thoroughly document the incident noting the source of the malicious code (if possible), resources impacted, and damage or disruption to information resources.

Related Statutes, Policies, or Requirements

Regulation 29.01.03

Contact Office

Contact The Texas A&M University System Chief Information Officer for standard interpretation or clarification.

OFFICE OF RESPONSIBILITY: The Texas A&M University System Chief Information Officer