SAP 29.01.03.T0.07 Information Technology Services – Malicious Code

Approved: May 4, 2006
Revised: May 21, 2014
Next Scheduled Review: May 21, 2019

Procedure Statement

This Standard Administrative Procedure (SAP) applies to all Tarleton State University network information resources.

The assessment of potential risks and the application of appropriate mitigation measures are to be determined by the information resource owner or their designee. In accordance with Texas Administrative Code 202 - Information Security Standards, each department and/or resource owner may elect not to implement some or all of the risk mitigation measures provided in this SAP based on information security risk management decisions and business functions. Such risk management decisions must be documented and reported to the designated information security officer (ISO).

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

Reason for Procedure

The purpose of the implementation of this SAP is to provide a set of measures that will mitigate information security risks associated with malicious code. There may also be other or additional measures that will provide appropriate mitigation of the risks.

Procedures and Responsibilities

1. PREVENTION AND DETECTION:

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

1.2 Where feasible, personal firewall software or hardware shall be installed to aid in the prevention of malicious code attacks/infections.

1.3. Email attachments and shared files of unknown integrity shall be scanned for malicious code before they are opened or accessed.

1.4 Storage devices will be scanned for malicious code before accessing any data on the media.

1.5 Software to safeguard against malicious code shall be installed and functioning on susceptible information resources that have access to the University network.

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

1.7 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.

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

2. RESPONSE AND RECOVERY:

2.1 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.

2.2 If malicious code is discovered, or believed to exist, the user will report issue to ITS staff for remediation.

2.3 The infected system shall be disconnected from the network to prevent further possible propagation of the malicious code or other harmful impact.

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

2.5 Due to the risk of possible backdoor code that could escape detection, ITS staff will determine the remediation steps necessary to recover from the incident.

2.6 Any removable writeable media recently used on an infected machine shall be scanned prior to opening and/or executing any files contained therein.

2.7 ITS staff 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

Supplements *SAP 29.01.03.T0.19 Security of Electronic Information Resources*

Definitions

1. **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.

2. **Information Security Officer (ISO):** responsible for administering the Tarleton information security functions and reports to the information resources manager (IRM).

3. **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 resources. 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**: Hidden malicious code inside a host program that appears to do something harmful.
   - **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.
   - **Spyware**: Software planted on a system to capture and reveal information to someone outside an individual's 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 targeted ads.
4. **Owner of an information resource**: an entity responsible for:
   - a business function; and,
   - determining controls and access to information resources supporting that support that business function.

Contact Office

Information Technology Services
Executive Director and CIO of Information Technology Services
254.968.9395