classification description: malicious code and activity essay sample

Technology, Computer

Base on the premise that there is a mix of computers running Windows 2000, Windows XP, Windows Vista, Windows 7, and Mac OS X, you must research and devise a plan to thwart malicious code and activity by implementing countermeasures and prevention techniques for dealing with viruses, worms, logic bombs, Trojan horses, and other related forms of intentionally created deviant code.

Introduction

Malicious software is written with the intent to damage or infect the system of Richman Investment. Malicious code or software is a threat to any internet-connected device or computer. The main goal of the attack is to affect one of the three information security properties which are Confidentiality, Integrity, and Availability. Confidentiality is affected if the malicious software is successful at disclosing private information. Integrity is compromised if the malware can modify database records either immediately or over a period of time. Availability is affected if malware can erase or overwrite files or inflict considerable damage to storage media.

SSCP® Domain Affected

Malicious Code and Activity

This domain examines the types of Malicious Code and Activities that can threaten the confidentiality, integrity, and availability of a system or information. The SSCP is expected to be familiar with the various types of Malicious Code and know how to implement effective countermeasures to prevent malicious code from operating. The SSCP should also know how to

detect, respond and recover from malicious activity on a system whether perpetrated by an internal or external entity and take steps to mitigate the risk of malicious activity.

Controls to Protect Against Malicious Code

Typical controls to protect against malicious code use technology, policies and procedures, and training, all applied in a layered manner from perimeters inward to hosts and data. The controls are of the preventative and detective/corrective variety. Controls are applied at the host, network, and user levels:

Host Level

* Host hardening, including patch application and security-minded configurations of the operating system (OS), browsers, and other network-aware software.

* Host IPS, including anti-virus, anti-spyware, and anti-rootkit can enable the hiding and surreptitious execution of malicious software code. An additional technology is software that limits applications calls to the OS to the minimum necessary for the application to function.

* Integrity checking software, combined with strict change controls and configuration management.

* Application of known-good configurations at boot-up.

* Periodic auditing of host configurations, both manual and automated.

Network Level

* Limiting the transfer of executable files through the perimeter.

* IDS and IPS monitoring of incoming and outgoing network traffic, including anti-virus, anti-spyware and signature and anomaly-based traffic monitors.

* Routing ACLs that limit incoming and outgoing connections as well as internal connections to those necessary for business purposes.

* Proxy servers that inspect incoming and outgoing packets for indicators of malicious code and block access to known or suspected malware distribution servers.

* Filtering to protect against attacks such as cross-site scripting and SQL injection.

User Level

* User education in awareness, safe computing practices, indicators of malicious code, and response actions.

Preventive Techniques

Network Users (including departmental staff on permanent, temporary, contract or casual tenure):

* Ensure they do not disable or interfere with the operation of antivirus software.

* Ensure corporate/education and TAFE personal computers/laptops in use are regularly made available for antivirus software updates.

* Exercise caution when opening email and related attachments.

* Do not download software from the Internet unless authorized by senior management and the technology support officer. Risks may include infringement of copyright in addition to introduction of malware or malicious code.

* Scan downloaded software for malware and malicious code.

* Do not develop, distribute or run any computer programs or code that is intended to replicate itself, cause damage, and/or impede the performance of any computer, software application or network whether malicious or otherwise.

* Immediately report malware and malicious code infection.

* Report incidents of security breaches in relation to incidents of malware and malicious code infection and any unusual related behavior to their immediate supervisor.

* Isolate infected computers from the network quickly to prevent further infection. To isolate the computer, either turn it off or disconnect the network cable.

* Scan all files and information contained on portable media and storage devices (such as DVDs, USB drives, floppy disks, etc.) for malware and

malicious code prior to being used on any department information systems (such as laptops, PDAs, desktop computers, etc.).

Definitions

Antivirus

Anti-virus software is used to prevent, detect and remove a range of malware, including computer viruses, worms, trojan horses, adware and spyware.

Computer Virus

Computer program that can copy itself and infect a computer. The term ‘ computer virus’ is sometimes used as a catch-all phrase to include all types of malware, including true viruses.

Malicious Code

A piece of unwanted computer software or code introduced into another program, attached to a document or exists on its own, for malicious purposes.

Malware

Short for malicious software, software designed to infiltrate a computer system without the owner’s informed consent. Usually refers to a variety of forms of hostile, intrusive, or annoying software or program code. Malware encompasses computer viruses, worms, trojan horses, spyware, dishonest

adware, crimeware, most rootkits, and other malicious and unwanted software.

Works Cited

Albright, J. G. (2002, March 2002). The Basics of an IT Security Policy. Retrieved from giac. org: http://www. giac. org/paper/gsec/1863/basics-security-policy/103278 Amsel, E. (2009, November 10). Information Security Policy. Retrieved from princeton. edu: http://www. princeton. edu/oit/it-policies/it-security-policy/ The IT Security Policy Guide. (2008). Retrieved from instantsecuritypolicy. com: http://www. instantsecuritypolicy. com/Introduction_To_Security_policies. pdf University: IT Security Policies. (2013, February). Retrieved from american. edu: https://www. american. edu/policies/upload/IT-Security-Policy-2013. pdf