Data Security

Student's Name
Institutional Affiliation

Threats and Vulnerabilities

Malicious software and attack types: Information Technology has many advantages that have eased information handling. However, the disadvantages are few but critical if information is to be stored safely. There are various categories of attacks related to malicious software. The common malware is a Trojan horse whereby it unconsciously requests the user to install in the operating system. Thereafter, the malware downloads other malware that help in corrupting files, sending information to remote servers and encrypting files. Elsewhere, rootkit is a malware that cannot be detected in the processes running because the programmer fears it will be uninstalled once noticed. Thus, the software remains concealed as it executes file corrupting activities and operating system modification. In some extremes, there are backdoors where an operating system does not require authenticating. To this end, the stored files are corrupted, and information easily retrieved.

It is recognized that all malware software can be prevented by installing security updates from the software manufacturer. The updates are mainly security based thus aiding in information security. In another sphere, booting the operating system from internal memory prevents data problems brought about by lack of authentication. Further, genuine programs are a guarantee against data storage problems such as corruption.

When designing an information handling system it is crucial to incorporate malware software that work to identify all malware installations in a computer for their legitimacy. The strategy ensures that there is real time protection and detection thus ensuring the necessary action is taken to eliminate the software. Elsewhere, the system should be installed with website security scans as well as eliminating over-privileged code in the system to boost information security.

User and Account Management and Training

In a bid to ensure essential security features are in place, identity management program is crucial. To this end, user role definitions where permission and access authorization are stated should be instigated. Elsewhere, password synchronization for various users is crucial to limit the number of users.

System passwords and need for authentication are controls to ensure risk related to accounting management and user.

Elsewhere, there are various recommendations that are put forward to ensure there is effective identity management program. Employees are crucial components because they use the system on a daily basis. Therefore, they should be the first to secure the system through use of appropriate operational skills such as installation of the right software and continuous use of genuine software. The system should also be continuously updated to ensure it is secure from malware and viruses.

An effective user awareness program involves understanding the easiest ways to fulfill and deliver the needed knowledge about system management in the most effective way. Listening to the different perspectives helps design detailed awareness materials. Elsewhere, the awareness message ought to be short and to the point by addressing organizational and individual concerns. The training program should cover different groups including new employees, infrastructure awareness for fresh network engineers, application awareness for specific system users and training for system managers. The process should be done on a continuous basis since there are many changes that affect system management.

Operating System and Application Security

Hardening refers to offering various methods of protection in data handling system. It involves installing firewall programs, closing certain ports, for example, server ports, disabling file sharing between programs and use of strong passwords.

There are various vulnerabilities associated with failure to harden systems including presence of unnecessary applications and services, running of unwanted software, presence of unnecessary logins and usernames and other unnecessary services.

To prevent such system problems, the system manager should install a patch to the kernel, for example PaX. Elsewhere, shutting open network ports, and use of firewalls secure the systems from such problems.

As a long-term strategy to prevent information from vulnerabilities related to hardening, tools such as Bastille Linux and Apache Hardener are used. The tools deactivate unnecessary features in configuration files thus acting as protective measures.