Securing Restricted Computers (ISSP-006)
Protecting computers that handle restricted data

Introduction

All computers connected to the network must be appropriately protected. Computers used at USF which contain information considered restricted require additional measures of protection. This document outlines the recommended steps local administrators must take during the initial setup and ongoing maintenance of such computers.

Requirements

Physical Security

Physical security is one of the most critical components of a security infrastructure. All of the items listed below can be implemented but would be worthless if someone is able to simply enter the room after hours and steal the entire computer.

Common solutions to improve the physical security of a room include installation of cameras, controlled access to authorized personnel only. Access to the server room can be controlled by card scanners or with a simple lock and key. Often the simple placing of signs alerting individuals that alarms and monitoring systems are in place are enough of a deterrent to stop thieves from robbing the facility.

Access Control List

Access Control Lists (ACL) are controls placed at the network level, instructing the network equipment used to connect a computer to the Internet to allow certain types of traffic from certain sources, while denying other types of access. Placement of ACL requires a detailed knowledge of the computer, its usage patterns, and the systems it accesses. Users of Point of Sale (POS) software should be able to obtain the information needed to implement ACL from their solution vendor. ACL is put in place by USF networking personnel. Contact the members of the Incident Response Team (IRT) for more details.

Encrypted Traffic

How does the data arrive to the computer? Is it sent or accessed anywhere else from your machine? Both inbound and outbound traffic must be encrypted if at all possible. If the data is accessed by entities through a web server installed on the machine, make sure you use a secure server. Avoid using email to send or receive the data at all cost.

Password Protection and Encryption

Often files containing restricted data are stored on a computer without any protection or encryption. Point of Sale systems, for instance, may store some credit card data locally to avoid loss of data in case of a network failure. Excel spreadsheets may be used to perform statistical analysis on student grades. Whenever it is necessary to store restricted files on a machine, these files must be protected by an authentication mechanism and/or encrypted.

Antivirus Protection

USF provides Symantec antivirus software to all computers free of charge. All USF machines must be equipped with antivirus software, whether or not they contain restricted information. In addition, the software must be set up to update its antivirus signatures on a daily basis. The software must be scheduled to run a Full Scan of the computer at least once a week.
Operating System and Applications Updates
Computers housing restricted information must be especially careful with updates. The operating system must be patched routinely, with the latest available security patches and service packs.

In addition to the operating system, all software applications installed on the machine, not only those involved with the restricted data in question, must be carefully monitored and maintained. This is a bit trickier than operating system patches. While most operating systems include programs that check for needed updates (Windows Updates on Windows OS, up2date or yum on Linux), not all applications include the same device. At times, maintaining software applications updated involve frequent visits to the application web site, or subscription to email lists. Examples of applications that must be kept updated include Adobe Acrobat and Flash Player.

Log Monitoring
Ensure that operating system and application logs are enabled and operating properly. Examine them often. If possible utilize automated software that monitors these logs and notifies you through email or paging of any anomalies.

Recommendations

Personal Workstations
Whenever possible, machines handling restricted information should not double up as personal workstations. User interaction may introduce uncertainties in the system (for instance, a user downloading and installing an unapproved Instant Messaging program), inadvertently allowing hackers to gain access to the system. User accounts on a restricted computer must be set up to only have those privileges needed to perform their job.

Firewall Software
An appropriately configured firewall product is similar to the ACL, controlling traffic in and out of the computer. Firewall software also provides the computer with additional logging capabilities that can examined routinely to unveil possible system breaches.

Several types of both hardware and software solutions exist, depending on your platform. The Symantec Antivirus Suite includes Network Threat Protection, with both a Host Based Firewall and Intrusion Detection system. Contact IRT for more details.

Backup or Development Machines
Often computers used as redundant servers, those used to backup the data, or those used during development are neglected. Development machines should not utilize restricted data, if at all possible. Otherwise, these machines must have the same security precautions as production machines. The same applies to those machines used as redundant servers or those used during the backup process.

Contact Information

For more details, contact the members of the Incident Response Team at (813) 974-2287, or email security@usf.edu.