Week 6 class discussions

Technology, Information Technology

Information Technology Security Information Technology Security Week 6 Discussion Cryptography means secrete writing (Coron, 2006). The main aim of cryptography is to protect the content of the message from unauthorized persons or programs. It ensures that communication between two devises happen securely over an insecure channel. Steganography means hiding of information in order not to be detected. It is advantageous to cryptography as the hidden message will not attract any audience. Watermarking involves embedding information to a host signal (Jiang, 2010). It operates with the principle of robustness to be safe against any attacks. Watermarking communication usually takes place in a one-to-many communication system while steganography communication takes place in a point-to-point communication. Both stenography and watermarking hide the content and existence of the message while cryptography hides the content but not the existence of the message, they are therefore mutually exclusive (Stefan & Fabien, 2000). Watermarking, cryptography, and stenography aim at securing messages from attackers.

The benefits of ADS outweigh the risks as files can be hidden on an NTFS hard disk in a way that is difficult to detect as long as there are proper security features to handle them and system administrators are aware of the streams. If Microsoft discontinues support of ADS in future versions of its operating system, the forensic industry would suffer a big blow as it would not be able to find most of the copies of some work for its forensic investigations. This is because streams are retained if a file is copied with ADS to another NTFS, which is very important for forensics.

Week 6 Discussion 2

The most significant obstacle to successful backing up data and/or recovering data for forensic investigators is lack of cooperation from the management (Wiles & Rogers, 2007). The management is responsible at providing funds and direction regarding backing up and recovering of data. However, due to many computer malpractices many managers get involved into, they fear that they might be caught one day when a forensic investigation is done and therefore might not fully cooperate in regard to backing up and recovering done for forensic purposes.

Forensic investigation is normally done to unearth the vices done in an organization. The results of forensic investigation are normally taken to law courts for legal actions to be taken. In the event that a system forensic is to be done, many people in the case normally do the much they can to destroy evidence in the computers. They do this through destroying computer systems, deleting information, burning computers, or even passing magnetic objects over hard disk with an aim of destroying any evidence (Vacca, 2008). If this is the case, such are information recovered and used for forensic investigations. Backup and recovery is therefore critical to the system forensics process to determine the potential effects on an investigation.

Week 6 Discussion 3

The physical security features observed include security guards, fencing including electric fence, alarm system, fire extinguisher, surge protectors, one door under lock, labeled equipment, locking the CPU, and placing backup sites away from the place of operation.

Week 6 Discussion 4

Information security threats at my house

My household information technology infrastructure will be vulnerable to the following threats: Virus attacks, password stealing, hardware and software theft, deletion of data, fire, and the power problems.

Protecting the system against the threats

The implementation will involve creating strong passwords, securing my house by locking it when not available, and installing antivirus software to protect the computer from malicious attacks, encrypting messages before sending, locking the CPU to prevent hardware theft components, using power surges and uninterruptible power supply, and fixing power extinguisher.

Reviewing and updating the plan

New threats emerge every day. The plan will therefore be reviewed and updated periodically to cater for new threats and any information technology infrastructure added at home.

References

Coron, J. S. (2006). What is cryptography? IEEE Security and Privacy, 4(1), p. 70-73.

Jiang, X. (2010). Digital watermarking and its application in image copyright protection. In 2010 International Conference on Intelligent Computation Technology and Automation, ICICTA 2010, May 11, 2010 - May 12, 2010. Changsha, China: IEEE Computer Society.

Stefan, K. & Fabien A. P. (2000). Information Hiding Techniques for Steganography and Digital Watermarking.

Vacca, J. R. (2008). Computer forensics: Computer crime scene investigation. New York, NY: Cengage Learning.

Wiles, J. & Rogers, R. (2007). Techno Securitys Guide to Managing Risks for IT Managers, Auditors, and Investigators. Security & Networking, Syngress, 1.