Incident handling procedures research paper

Law, Criminal Justice

Incident Handling Procedures

In this modern age of technology, people, businesses and government agencies rely on computers for day to day operations in their area of work. Information technology has open doors to quick and easy access of information that any individual might find interest in (Vacca, 2009, p. 150). This advancement has numerous advantages including convenience, efficiency and reliability of information access to assist in education, research, work and leisure related activities. Information technology has however opened a door for malicious people who are bent on ruining the success, image and reputation of individuals or corporate entities through unauthorized access, known as hacking, of servers and computers bearing sensitive information for the sake of extorting money from the victims or using the information to their advantage at the expense of the victims (O'Brien & Yar, 2008, p. 171).

The immediate action to take after a network attack is to identify the type of attack. The attack is identified by its characteristics. Once the attack is identified, then it can be properly contained. In containing the attack several steps have to be taken to protect the other systems and networks from being damaged (Northcutt, 2003, p. 5). This second step facilitates the stoppage and neutralization of the attack. The third and final step is known as recovery and analysis; this involves the recovery of lost data and information as well as the analysis of the extent of damage and losses incurred in terms of data and finances, which loopholes facilitated the attack, how well the attack response was handled the current status of the network after attack, and finally how to be prepared to prevent and handle future

network attacks (Guttman & Roback, 1995, p. 133). The assumption made in responding to this attack is that the network attack was instigated by a third party and was not an internal sabotage.

Protection from an attack should be well planned out through careful analysis and preventive measures. A computer emergency response team should be set up in large firms and government agencies to be able to effectively handle and respond to any network attacks in a professional way (Santos, 2008, p. 35).

REFERENCES

O'Brien, M. & Yar, M. (2008). Criminology: The Key Concepts. New York: Routledge.

Vacca, J. (2009). Computer and information security handbook. Massachusetts: Morgan

Kauffman Publishers.

Guttman, B., & Roback, E. (1995). An Introduction to Computer Security. Georgia: Kaufmann

Publishers.

Northcutt, S. (2003). Computer Security Incident Handling: An Action Plan for Dealing with

intrusions, Cyber-and Other Security-Related Events. Maryland: SANS Institute.

Santos, O. (2008). End-to-end network security: defense-in-depth. Texas: Cisco Press.