Post network intrusion procedures research paper sample

Business, Company

Post Network Intrusion Procedures

Most organizations use networked systems in which computers are interconnected so as to share company resource and have a well management Information Systems base. This network is mostly connected to the internet, described by the computer science experts as a ‘ Hostile Network’. Connection to the internet exposes the network to attacks either by malicious or non malicious attackers. They can do so in many ways such as dictionary attacks, brute force and distributed attacks using code such as Trojans . It is therefore inevitable to face such intrusions and it is upon the administrators of the network to detect such an intrusion and develop a structure of how to recover from such an intrusion.

An organization has to develop a network breach procedure that confirms the security breach and at the same time accumulate the extent of the damage caused by the breach. According toLee (1999), such a response to an intrusion could be divided in three parts. The first part is the Information Systems’ Security response, then the Information Technology response then finally the Law Enforcement response.

The information systems’ response to an external access seeks to analyse the extent to which the intrusion has curtailed the confidentiality and integrity of the information in the system. Some of the procedures include; evaluating the extent of the information accessed, evaluating system logs that have been affected, determine if other systems of the organization have affected and finally recommend to the management new security measures to safeguard the data .

The second procedure is to determine the extent to the intrusion has

affected the Information technology (IT) part of the organization. The managers should evaluate the effect of the intrusion on the software and hardware of personal computer and servers of the company. Remove any alien code and restore system configurations.

Finally, seek methods and ways of identifying and prosecuting the perpetrators of such an intrusion. The Federal Bureau of Investigations (FBI) is mandated to handle computer crime. This might help restore confidently and integrity of the information system as well as prevent future attacks

References

Bouillet, E., & Ellinas, G. (2007). Path routing in mesh optical networks. John Wiley & Sons.

Cole, E., Krutz, R., & Conley, J. (2007). Network security fundamentals. John Wiley and Sons.

Lammle, T. (2006). CCNA INTRO: Introduction to Cisco Networking Technologies Study Guide: Exam 640-821. John Wiley & Sons.

Lee, D. (1999). Enhanced IP services for Cisco networks. Cisco Press.

Vasseur, J.-P., Pickavet, M., & Demeester, P. (2004). Network recovery: protection and restoration of optical, SONET-SDH, IP, and MPLS. Elsevier.

Vladimirov, A., Gavrilenko, K., & Mikhailovsky, A. (2005). Hacking exposed Cisco networks: Cisco security secrets & solutions. McGraw-Hill Prof Med/Tech.

.