Ids policy

Running head: IDS Policy IDS Policy Affiliation December 2009 Computers are powerful devices that assist people to store information and carry out operations on huge amounts of data quickly. Almost every firm, regardless of size, utilizes computers to handle bookkeeping, track inventory, and store documents. However, when businesses grow, they often need several workers to enter and process data at the same time. For this to be beneficial, those workers must be capable to share the data each person enters. As a result, networking computers becomes essential. Networks are merely a group of computers linked by cable or other media so they can share information (Nash, 2000). Also, there are different evils associated to these network structures. For instance, personal information theft, business information hacking and virus attacks are the contemporary issues businesses are facing nowadays in the network communication and data transfer areas (Frederick, 2002). Furthermore, because of the increasing amount of intrusions the local networks and Internet have turned out to be uncertain, therefore, businesses more and more applying a variety of systems that monitor information technology security breaches (Sans, 2009).

Network intrusion as its name represents, attempts to recognize attempted or applied intrusions into network and to carry out proper actions for the intrusions. Intrusion detection includes an extensive collection of methods that differ on several axes. A few of these axes comprise: (Silberschatz, Galvin, & Gagne, 2004)

The time period that detection takes place: in real time (while it is taking place) or following the information only.

The types of input inspected to identify intrusive action. These could

comprise user shell commands, process system calls, as well as network packet headers or contents. Several types of intrusions might be identified only by correlating information from various such sources.

The variety of action capabilities. Basic and straightforward types of actions consist of changing an administrator of the possible intrusion or in some way halting the potentially intrusive action, for instance, killing a course of action engaged in actually intrusive activity. In a complicated type of action, a system might clearly redirect an intruder’s action to a trap. A false resource exposed to the attacker with the aim of observing and gaining information about the attack; to the attacker, the resource appears real.

These levels of freedom in the design of space for detecting intrusions in systems have brought an extensive variety of solutions acknowledged as intrusions detection systems (IDS) (Silberschatz, Galvin, & Gagne, 2004).

Gem Infosys desires to protect the business network and organizational business resources. The main aim and objective of this policy is to offer procedures to set up security monitoring and intrusion detection to defend business resources as well as data on the organizational network. Gem Infosys policy is intended to protect both the privacy of business data that can be stored on the Gem Infosys computer as well as to shield the managerial network as of being infected through some hostile software that can be approached from the broadband connection to the Internet. This IDS policy as well cares for the business network access for different users in the corporate (Comptechdoc, 2009).

Scope

This Gem Infosys IDS policy covers each network host on the business network as well as the whole data business network comprising each path

through which business data can travel. The main goal behind this policy implementation is to protect the system from the outer assaults on the corporate network. Also, another aim is to establish a security plan that addresses all the aspects of the security such as internal and external security management (windowsecurity, 2009).

IDS Policy Parameters

The main objective of the IDS policy for the Gem Infosys is:

1. Enhancing the security level internally and externally to the business.
2. Preventing un-authorized system entrance
3. Preservation of the business data
4. Establishing integrity of the business information
5. Establishment of appropriate security parameters to stop external intrusions
6. Permitting access only to authorized users
7. Detection and handling of any suspected network intrusion

Conclusion

This paper has presented detailed analysis of the IDS policy for the Gem Infosys. This paper has presented detailed overview of the different aspects and parameters of the IDS policy and operating structure. Through the implementation of this IDS policy Gem Infosys can protect the overall network form outer attacks.

Bibliography

Bradley, T. (2009). Introduction to Intrusion Detection Systems (IDS). Retrieved 09 28, 2009, from http://netsecurity. about. com/cs/hackertools/a/aa030504. htm

comptechdoc. (2009). Intrusion Detection Policy. Retrieved 11 30, 2009,

from http://www. comptechdoc. org/independent/security/policies/intrusion-detection-policy. html

Comptechdoc. (2009). Network Intrusion Detection. Retrieved 09 28, 2009, from http://www. comptechdoc. org/independent/security/recommendations/secintdet. html

Frederick, K. K. (2002). Evaluating Network Intrusion Detection Signatures, Part One. Retrieved 09 29, 2009, from http://www. securityfocus. com/infocus/1623

McHugh, J., Christie, A., & Allen, J. (2009). The Role of Intrusion Detection Systems. Retrieved 11 30, 2009, from http://docs. google. com/viewer? a= v&q= cache: JF9VTOoAi4kJ: www. cert. org/archive/pdf/IEEE_IDS. pdf+Intrusion+detection+system+policy&hl= en&gl= pkπd= bl&srcid= ADGEESi9UDrh-HKO1pD6QhLg6kS-xxjGt6thfSESMGledGaFoFGyhKNRV34nX7VkHU1uBDM9KH7OEHTGldkX8CY8Q7YUEimxxdFmq0o

Nash, J. (2000). Networking Essentials, MCSE Study Guide. California: IDG Books Worldwide, Inc.

Sans. (2009). Intrusion Detection FAQ: What is Intrusion Detection? Retrieved 09 28, 2009, from http://www. sans. org/resources/idfaq/what_is_id. php

Silberschatz, A., Galvin, P. B., & Gagne, G. (2004). Operating System Concepts (7th Edition). New York: Wiley.

windowsecurity. (2009). Intrusion Detection Systems (IDS) Part I - (network intrusions; attack symptoms; IDS tasks; and IDS architecture). Retrieved 11 30, 2009, from http://www. windowsecurity. com/articles/Intrusion_Detection_Systems_IDS_Part_I__network_intrusions_attack_symptoms_IDS_tasks_and_IDS_architecture. html