Ids policy

RUNNING HEAD: INTRUSION DETECTION SYSTEM Intrusion Detections System of the of the Intrusion Detections System

Introduction

A well define thought and planning for Gem Infosys is necessary before installing an Intrusion Detection System (IDS) on a network. Besides technical issues and product selection another serious factor are the resource issues that includes manning the sensor feeds, product expenses and infrastructure support that must also be kept in mind.

Basically the IDS help in recognizing and observing the intrusion attempts made by any internal or outside party into the organization's network. These systems are made to spot the threats and then take suitable measure to remove them.

Discussion

Basically there are two types of IDS

1. Host based IDS: These are systems that are typically installed on the host systems that are planned to monitor. These systems could be any workstation, server or other network peripherals such as a router. The IDS system runs as a service or a process and has the ability to detect the network traffic on the host system. To save the system from past threats a " threat signature" database is present to make sure that the system is not vulnerable to those threats. Microsoft, Cisco and Tripwire etc. are some of the companies that deal in these IDS systems. (Spafford, Zamboni, 2000)

2. Network Based IDS: These are systems that confine and analyze packets on the wire. Network based IDS are used to protect the entire systems on the network unlike Host base IDS which are built for a single system. After confining the packets on the network they send it to the IDS console for

inspection. Major vendors include Cisco and Symantec.

Setbacks with IDS solutions

As Gem infosys is a small software company having just 10 PC's and a broadband connection should not face much difficulty with the IDS system. But sometimes IDS solutions can bring out bogus alarms that may result in incorrect distribution of information. Inadequate potential and bad configuration choices are the major factors for this kind of problem. On the other hand many products need to be kept updated and well managed to avoid problems such as well updated sensors.

Developing an IDS Policy

In the pre deployment stage when Gem Infosys is installing an IDS a policy needs to be designed in order to make sure that responsibilities and processes are well defined.

Procedures will be maintained for recognizing the security threats. Incidents will be classified as " non-serious" or " serious". If there is a problem of failing hardware, target network administration should be fully responsive that if network taps are used, even fail safe taps can take up to a second to re-negotiate with the interfaces and could upset the services. (Liepins, Vaccaro, 1992)

Non-serious incidents policy

When devising the policies Gem Infosys should know that Non Serious incidents include those activities in which the attack or threat is not purposely directed at the organizations network.

It should also be analyzed that no sensitive data or information is revealed or used in an illegal manner or without any authorization.

Serious Incidents Policy

Those activities in which the attack or threat is purposely directed at the organizations network.

Sensitive data or information is revealed or used in an illegal manner or without any authorization.

All the networking and IT staff of Gem Infosys will report any possible security event that they come to know to the assigned security officer. Any activity or breach of security policy is a security incident. The organization will maintain a set of rules and procedures when dealing with these kinds of security incidences.

All the incidents that are mentioned as serious by the security officers will be at once conveyed and reported to all the top level management and the concerned authorities.

The organization will try to alleviate any damaging effects, when possible, if a security incident affects customer information.

Conclusion

Confidence gaining of the network's staff is essential to a successful setting up of an IDS system. The network and system administrator's views and concerns should always be given importance as they are managing the whole network of Gem Infosys and have a better view of the whole scenario. Gem infosys should try to win the hearts and minds of all the network staff and in return the company will get a good threat free network.

References

Liepins, G. E.; Vaccaro, H. S.: Intrusion Detection: It's role and validation, Computers & Security 11/1992, 347 - 355

Spafford, E. H.; Zamboni, D.: Intrusion detection using autonomous agents, in Computer Networks, Volume 34, Issue 4, October 2000, 547-570