Security network intrusion detection system (ids)

Network Intrusion Detection System Introduction Intrusion detection and prevention is vital when it comes to a network's security. A network intrusion detection system (NIDS) keeps a check on the network traffic, signals when it encounters a security breach, a malicious activity or an attack, and obstructs the source IP address from accessing the network. Below is discussed a case study and important actions which become necessary in case of network intrusion.

Case Study

If I get an alert from the IDS telling me that somebody is trying to connect repeatedly to port 3389 of my computer at 192. 168. 2. 124 and the mouse pointer starts moving by itself, I would carry out the following steps.

1) The first and foremost thing is to have a grip upon the mental approach. I would try to stay composed and relaxed rather than getting panicked. I would analyze the whole situation cool mind. Whenever a network is established, problems like these are likely to occur and companies always have a well organized solution for this. So, there is no need to get horrified.

2) Under such a situation, it becomes important to isolate the affected computer immediately. An affected machine on a network can cause all other machines on that network to be affected. I would unplug the cable and then disconnect the affected computer both from the internet and the network. This way, the intruder will not be able to have an access to the machine nor will he be able to attack other computers on the network by means of the affected one.

3) I would block the port 3389 temporarily. TCP port 3389 is the Remote Desktop Protocol (RDP) that enables a user to connect to a computer on a network. I will find out if VPN (virtual private network) had been established

to protect the RDP or port 3389 traffic. I would make arrangements for the establishment of site-to-site VPN tunnel before reconnecting the computer to the network so as to secure the RDP traffic from Address Resolution Protocol (ARP) poisoning (Savill, 2008). Further investigations include: Were there passwords and sensitive information saved on the computer like ISP access passwords? These must be changed at once. How long has the intrusion gone undetected? The chances of co-computers on the network being affected increase with the time the affected one keeps on working on the network. I would investigate if the computer had updated anti-virus and desktop firewall software installed. I would make backups of all sensitive information and format the operating system. Then, I will reload the sensitive information from backup files while scanning them for viruses.

4) Whenever a security breach like this occurs, the network administrator is the first to be informed. However, it is important to inform all the operators who are dealing with the network.

5) It would be necessary to have a review of firewall and IDS logs so as to have an idea if there was a problem with firewall and IDS settings. I would see if the operating system of the affected computer hosted the firewall module station which “ is a key part to securing the firewall” (Spyders Inc., 2007). I would check the IDS logs to make sure that the security needs were being met or not. I would check whether or not there was a software firewall installed on the computer in combination with a hardware firewall connected to the modem because using the combination not only blocks unwanted attacks from outside but also stops malware from getting out if the system becomes infected (DIY Online Security, 2007).

Conclusion

To sum up, it is very important to get the affected computer isolated from the network and then have it checked as to what caused the intrusion possible by reviewing the firewall, IDS logs and anti-virus updates, and investigation about serious concerns should be carried out.

References

DIY Online Security. (2007). Isolate your computer system from the internet. Basic Computer Security. Retrieved from http://www. diyonlinesecurity. co. uk/base/bcs/isolate. html

Savill, J. (2008, February 04). The dangers of using RDP without a VPN. WindowsIT Pro. Retrieved from http://windowsitpro. com/article/articleid/98208/the-dangers-of-using-rdp-without-a-vpn. html

Spyders Inc. (2007). Firewalls with Application Intelligence. Security Solutions. Retrieved from http://www. spyders. ca/firewall. php#