Free securing windows essay example

Law, Security

The establishment of an audit policy is an essential feature of security. The monitoring of the modification or creation of objects allows a network security administrator to track probable security problems, enabling him or her to guarantee user accountability and offering evidence in the occurrence of a security violation or breach. In order to ensure such security superiority in the organization, a number of events should be audited. In auditing them, windows will keep records of the events in the security log found in the event viewer. These events include account logon events, account management, directory service access, logon events, object access, policy change, privilege use, process tracking and system events.

Logon events and object access should also be audited to determine if a user has logged on or off one’s computer and to check if an individual has used a folder, file, printer or any other object. This will be implemented on the database servers and the other servers. Lastly, the policy change, privilege use, process tracking, system events should be audited to determine if there are any attempts to change the local security policies, to determine the rights of users, to check the occurrence of events or to monitor system events such as shutting off, restarting or when a program or process attempts to undertake an activity which is not permitted.

Apart from the window-enable auditing, it is important to implement network intrusion detection system (NIDS). It is imperative to have a NIDS which identifies as many intrusions as possible while limiting the quantity of false alarms. However, there is no one single NIDS which can be deployed to detect all potential network-based attacks. Therefore, a system which combines various technologies to detect several types of attacks may achieve the desired result. This would involve detecting any potential intrusions using protocol anomalies, stateful signatures, back door detection, traffic anomalies and lastly pattern matching utilizing regular expressions(Frincke, 2002). A good example of such a host-based system is the Juniper Intrusion Detection and Protection system. Although not perfect, file integrity checker system may be used to gather evidence of an attack or unauthorized changes to the system.

Having an accurate hardware and software inventory for each system is important for Cyber Security because it collects a detailed information of the hardware and software characteristics of the client in a hierarchy; taking note of various information such as running process, O. S, peripherals, services and so forth which run on the client computer (Meier, 2003). As a result it aid in monitoring the states of each computer in the network, making it easier to maintain a desired security standard across the network.

References

Frincke, D. A. (2002). Intrusion detection. Amsterdam: IOS Press.

Meier, J. D. (2003). Improving web application security: threats and countermeasures. O'Reilly Media, Inc..