Defense in Depth

Defense in Depth

Defense in depth is a defense mechanism which confronts different attack methods through multi-layered network security architecture. It is safer and more secure compared to a single defense mechanism.

The Concept of Defense in Depth

The concept of defense in depth originates from the military discipline. Defense in depth aims at stalling intruders' attack in order to buy time for military deployment.

In a computer network, defense in depth not only intercepts intruders' attacks on the network but also buys time for a system administrator to inspect and repair the systems, thereby reducing the chance of a successful invasion and the subsequent impact.

Setup and Operation of Defense in Depth

The following is a simple example of the setup of defense in depth:

The setup of defense in depth normally starts from an organisation's Internet gateway, which is externally connected to other networks such as the Internet and internally connected to the organisation's internal network. It extends all the way to the secured installation of internal servers and users' computers. It usually includes two layers of firewalls, the Demilitarised Zone (DMZ), an Intrusion Detection System (IDS) and anti-virus software, etc.

The vanguard defending the whole network is the outer firewall. The outer firewall, such as packet filtering firewall, has a function to resist frontline attacks from external networks. It filters each incoming and outgoing packet according to predefined policies in order to determine whether the packets are allowed or denied to get in or out of the network.

In between the two layers of firewalls is the DMZ, which separates the internal and external networks. The servers that allow external access, such as web servers, are placed here. It can prevent direct access from external networks to the internal network.

The DMZ normally includes an IDS to detect attacks directed to this zone. The IDS can send out warnings and reports when any signal of intrusion is detected. This allows a system administrator to discover an attack as early as possible and perform inspection and repair tasks in time.

Following DMZ is the inner firewall. Inner firewall and outer firewall should be acquired from different suppliers. This prevents attacks to the same potential security loopholes in these firewalls.

Different from the outer firewall's sole function to filter packet, the inner firewall takes further steps to inspect the information within the packet and decide whether the connection of that network service is allowed or denied based on the packet's source and destination IP addresses, port number and the service requested.

To go deeper in the setup is the internal network. Normally, internal servers and users' computers are installed with firewall and anti-virus software with the latest virus signature for further protection.

In conclusion, even if an intruder can exploit the security loopholes of the outer security layer, the next layer of security measures will provide appropriate defense and alert.

The security measures of each layer are implemented using different functionalities and technologies to resist intruder's attacks and consequently protect important information in the system.

To learn more about information security, please visit the InfoSec website at:

http://www.infosec.gov.hk