3.6 Telecommunications

A website hosted in a tightly protected network is suddenly defaced. The log files do not show any record of intrusion. How did the cracker managed to break into the highly secured network?

3.6.1 Backdoor Access to Sabah.Net

Policy Any connections that may establish a backdoor access to Sabah.Net is strictly prohibited.

Standard No backdoor access is allowed and any existing backdoor must be removed.

Procedure

(1) All modems should be disabled or removed from desktop computer(s) which are connected to Local Area Networks (LAN).

(2) Any desktop computer(s) that is/are found to have accessed the internet through back door access i.e. not via SabahNet must be disconnected and verified by ICT personnel to be clean before reconnecting to network.

(3) All computers must have the most recent security updates, operating system patches, and antivirus patterns. For notebook computers, they must be installed with firewall.

(4) Any unnecessary program(s) and service(s) which are not required to perform official job should be removed from computers to minimise risk of being compromised by malware or hacker.

Guidelines

(5) Backdoor is a hardware or software-based hidden entrance to a computer system that can be used to bypass the system's security policies.

(2) Backdoor connections include all non Sabah.Net access (e.g dial up access, broadband, leased line, wireless, etc).

(3) Clean is defined as free from malware. Malware include but not limited to all types of viruses, worms, trojan horses, spywares, adware etc.

(4) Security updates refer to any updates and hotfixes for any software used.

(5) Firewall for notebook computers may include built-in firewall and the approved software list at http://www.sgCERT.org/software