3.7 Webservers

What if a picture in the State webserver is replaced with a pornographic picture by a hacker, and even after restoration, the incident recurs?

Audience System administrator

Policy All webservers should be secured to prevent any possible compromise and/or cyber attack.

Standard Latest security measures should be applied to webservers, including all applications and services residing in them.

Procedure

The system administrator, unless otherwise indicated, must implement security measures and controls including, but not restricted to the following:

(a) Install software patches and/or upgrades as soon as they are available and successfully tested;

(b) Harden and lockdown the operating system and applications;

(c) Install antivirus software and update it as soon as new versions and/or patterns are available;

(d) Validate all on-line input;

(e) Conduct web security scans at least once a month;

(f) Enable full web service logging;

(g) Closely monitor for any possible attack or compromise;

(h) Immediately report any attempt, or successful attack or compromise to Incident Response and Forensic Team;

Guidelines

1. For detailed procedure on testing, please refer to Systems Documentation Policy (3.1.2).

2. Hardening and lockdown include, but not restricted to implementing strong passwords and disabling unnecessary services.

3. Applications and services include, but not restricted to operating systems, web services and device drivers.

4. Software patches include, but not restricted to patches for operating systems, web services and device drivers.

5. Web security scans include, but not restricted to web scans and Common Gateway Interface (CGI) scans.