NHS CFH Infrastructure Security Team (NHS CFH IST)

NHS
Connecting for Health

# Web Server Security

When setting up a web server, there are a number of good practices in relation to securing such servers which should be followed. The list provided here by the Infrastructure Security Team (IST) should not be considered exhaustive but as a starting point for securing such servers. The list is in no particular order of importance. Please send any requests for further information to the IST mailbox at: cfh.infosecteam@nhs.net

1. Ensure that the web server is appropriately isolated. This is usually achieved by use of a De-Militarised Zone (DMZ). For a web server which contains high risk or sensitive information, consider placing the server in its own subnet or VLAN. Good practice advice can be found on the IST Good Practice Guidelines web page [1].

2. Ensure that any firewall which is used to protect the web server only allows inbound access to the relevant services on the web server. Ensure that any rules which allow the web server to communicate outbound are appropriate and needed for correct operation of the web server.

3. Ensure that all appropriate patches are applied to both the host operating system, the web server software itself and any applications which are running on the web server. Implement a patch management regime and stay up to date with manufacturers notifications on patches and monitor security web sites and security mailing lists which provide information on newly discovered web server vulnerabilities. Suggested links and resources can be found on the IST website [2]

4. Disable (or remove if possible) all unneeded services and user accounts on the web server. In addition, to further protect ('harden') the server, implement any web server side security protections provided by the vendor of the web server software. For Microsoft IIS, ensure that IISLockdown and URLScan are implemented and appropriately configured. For Apache (and related web server software), implement and configure mod_security.

5. For web servers hosting active content or content which interacts with the user or takes input from the user, consider the advice and guidance provided by the OWASP project [3]. This guide provides information on the top ten web application security vulnerabilities and how best to avoid them.

6. Ensure that the web server is regularly penetration tested by a CHECK or CREST approved 3rd party and that any discovered vulnerabilities are actioned appropriately after a suitable risk assessment.

References

[1] - http://nww.connectingforhealth.nhs.uk/infrasec/gpg/
[2] - http://nww.connectingforhealth.nhs.uk/infrasec/information/
[3] - http://www.owasp.org/index.php/Top_10_2007