INFORMATION SECURITY POLICY

INFRASTRUCTURE HARDENING POLICY

ISO 27002	12.6.1
Author:	Chris Stone
Owner:	Ruskwig
Organisation:	TruePersona Ltd
Document No:	SP-12.6.1
Version No:	1.0
Date:	6th September 2010

Document Control

Document Storage

Document Title Hardening Policy
Document Location C:\www\Ruskwig\docs\iso-27002\Infrastructure Hardening Policy - RW.doc

Version History

Version No	Version Date	Author	Summary of Changes
1.0	06/09/2010	Chris Stone	First Issue

Approvals

Name	Title	Date of Approval	Version No
Chris Stone	Director	06/09/2010	1.0

Distribution

Name	Title	Date of Issue	Version No
Everyone	Internet	06/09/2010	1.0

Contents

0. Overview

0.1 Hardening is the process of securing a system by reducing its surface of vulnerability. By the nature of operation, the more functions a system performs, the larger the vulnerability surface.

0.2 Most systems perform a limited number of functions. It is possible to reduce the number of possible vectors of attack by the removal of any software, user accounts or services that are not related and required by the planned system functions. System hardening is a vendor specific process, as different system vendors install different elements in the default install process.

0.3 The possibility of a successful attack can be further reduced by obfuscation. By making it difficult for a potential attacker to identify the system being attacked the attack can not easily exploit known weaknesses.

1. Purpose

1.1 This policy defines the procedures to be adopted for infrastructure hardening.

2. Scope

2.1 This policy applies to all components of the information technology infrastructure and includes:-

- Computers
- Servers
- Application Software
- Peripherals
- Routers and switches
- Databases
- Telephone Systems

2.2 All staff within the IT Department must understand and use this policy. IT staff are responsible for ensuring that the IT infrastructure is hardened and that any subsequent changes to systems do not affect the hardening of systems.

3. Risks

3.1 Without effective hardening there is an increased risk of the unavailability of systems. This can be caused by attackers, viruses and malware exploiting systems.

3.2 If external systems such as web servers and email servers advertise their type and version, it makes it easier for an attacker to exploit known weaknesses.

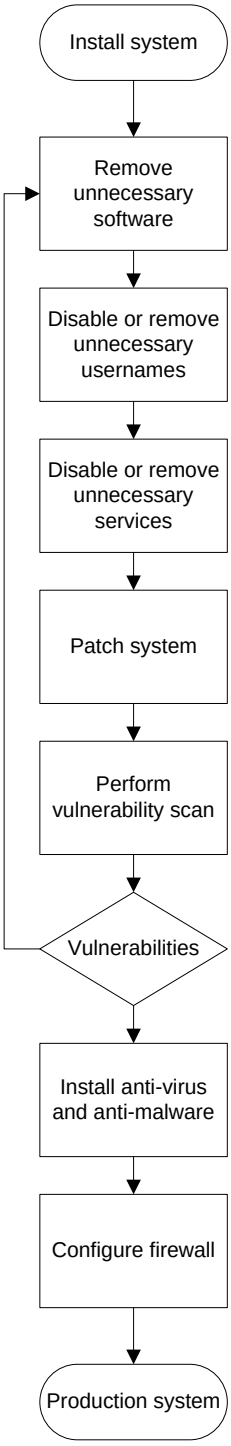
3.3 Systems which run unnecessary services and have ports open which do not need to be open are easier to attack as the services and ports offer opportunities for attack.

4. Policy

4.1 The organisation's IT infrastructure will be hardened according to this policy to minimise vulnerabilities.

4.2 Hardening Process

4.2.1 All new systems will undergo the following hardening process.



The process steps are as follows.

4.2.2 Install System

4.2.3 Install the systems as per the vendor's instructions.

4.2.4 Remove Unnecessary Software

4.2.5 Most some systems come with a variety of software packages to provide functionality to all users. Software that that is not going to be used in a particular installation should be removed or uninstalled from the system.

4.2.6 Disable or Remove Unnecessary Usernames

4.2.7 Most systems come with a set of predefined user accounts. These accounts are provided to enable a variety of functions. Accounts relating to services or functions which are not used should be removed or disabled. For all accounts which are used the default passwords should be changed. Consideration should be given to renaming predefined accounts if it will not adversely affect the system.

4.2.8 Disable or Remove Unnecessary Services

4.2.9 All services which are not going to be used in production should be disabled or removed.

4.2.10 Patch System

4.2.11 The system should be patched up to date. All relevant service packs and security patches should be applied.

4.2.12 Perform Vulnerability Scan

4.2.12 The system should be scanned with a suitable vulnerability scanner. The results of the scan should be reviewed and any issues identified should be resolved.

4.2.13 Vulnerabilities

4.2.14 If there are no significant vulnerabilities the system can be prepared for live use.

4.2.15 Install Anti-Virus and Anti-Malware

4.2.16 A suitable anti-virus and anti-malware package should installed on the system to prevent malicious software introducing weaknesses in to the system.

4.2.17 Configure Firewall

4.2.18 If the system can run its own firewall then suitable rules should be configured on the firewall to close all ports not required for production use.

4.2.19 Production System

4.2.20 The system is now ready for production use.

4.3 Hardening Requirements

4.3.1 Only software that has been approved for use by the IT department may be installed on the organisation's computing devices.

4.3.2 Non-essential software applications and services will be uninstalled or disabled as appropriate.

4.3.3 Servers, PC's and laptops will be configured to prevent the execution of unauthorised software.

4.3.4 Vulnerability scanning and inventory scanning software will be configured to automatically uninstall unauthorised software.

4.3.5 Bios passwords will be implemented on all PCs and laptops to protect against unauthorised changes.

4.3.6 The boot order of PC's and laptops will be configured to prevent unauthorised booting from alternative media.

4.3.7 All PC's and laptops will be built from a standard image. Any change to the standard image must be supported by a business case.

4.3.8 Access to the local administrator account will be restricted to members of IT Department to prevent the installation of unauthorised software and the modification of security software and controls.

4.3.9 Default passwords will be changed following installation and before use in a production environment.

4.3.10 All PC's and servers will be protected by anti-virus and anti-spyware software. The anti-virus and anti-spyware software will be configured to automatically download the latest threat databases.

4.3.11 A local firewall will be installed on all PC's and laptops. The firewall will be configured to only allow incoming traffic on approved ports and from approved sources.

4.3.12 The use of removable media will be controlled. Removable media will be controlled by endpoint protection software.

4.3.13 All servers must pass a vulnerability assessment prior to use. The servers will be scanned using the organisations vulnerability scanning tools. All network and operating system vulnerabilities will be rectified prior to use.

4.3.14 Public facing servers will be further hardened by obfuscation. The headers on web servers and email servers will be changed so that it is not immediately apparent what software they are running.

4.3.15 All devices on the organisation's network will be scanned for vulnerabilities every 3 months. Any issues identified will be reviewed and rectified as appropriate.

4.3.16 All devices on the organisation's network will patched in accordance with the Technical Vulnerability and Patch Management Policy.

5. Enforcement

5.1 If any member of IT staff is found to have breached this policy, they may be subject to disciplinary action.

5.2 Any violation of the policy by a temporary worker, contractor or supplier may result in the termination of their contract or assignment.