INFORMATION SECURITY GUIDELINE

UBC Systems & Application Hardening Guides

Introduction

1. Hardening guides are meant to further enhance the levels of security for systems, applications, databases and devices by reducing the exposed attack surface of a product or service. Application of these guides requires some vigilance as they could also render systems, applications, or databases unusable for their intended purpose.
2. This guideline has been issued by the Chief Information Officer to supplement the Vulnerability Management standard. Compliance with this guideline is recommended, but not mandatory. Questions about this guideline may be referred to information.security@ubc.ca.

Available Guides

3. The following hardening guides are available via the Centre for Internet Security (CIS):

Category	Available Guides	Link
Operating Systems	Linux, Novell Netware, Unix, Microsoft Windows	http://benchmarks.cisecurity.org/downloads/browse/index.cfm?category=benchmarks.os
Databases	IBM DB2, Microsoft MS SQL, MySQL, Oracle, Sybase	http://benchmarks.cisecurity.org/downloads/browse/index.cfm?category=benchmarks.servers.database
LDAP	Novell eDirectory, OpenLDAP	http://benchmarks.cisecurity.org/downloads/browse/index.cfm?category=benchmarks.servers.ldap
Network Devices	CheckPoint Firewalls, Cisco Devices, Juniper Devices, Wireless Network Devices	http://benchmarks.cisecurity.org/downloads/browse/index.cfm?category=benchmarks.network
Mobile Devices	Google, Android, Apple	http://benchmarks.cisecurity.org/downloads/browse/index.cfm?category=benchmarks.mobile

4. The CIS guides are configured into two categories: Level 1 & Level 2 controls:
   a. Level 1 controls are generally safe settings that should be configured at a minimum on a server or a database, and should cause little or no interruption of service; and
   b. Level 2 controls are recommended in highly secure environments and carry a higher risk of impacting services.
5. WordPress and Drupal are popular content management systems and are frequently targeted for attacks; as such it is recommended that the Securing WordPress and Securing Drupal guidelines be used in hardening and protecting WordPress and Drupal deployments.

Related Documents

Policy SC14, Acceptable Use and Security of UBC Electronic Information and Systems
Vulnerability Management standard
Securing Drupal guideline
Securing WordPress guideline