CMSGu2012-09

National Computer Board

Mauritian Computer Emergency Response Team

Enhancing Cyber Security in Mauritius

CERT-MU

Technical Guideline on Public Internet Access Points (Computer-Clubs, Cyber-Caravans, Post-Offices)

November 2012

Table of Contents

Contents

DISCLAIMER: *This guideline is provided for informational purposes only. Information in this guideline, including references, is subject to change without notice.*

The products mentioned herein are the trademarks of their respective owners.

1.0 Introduction

1.1 Purpose and Scope

This guideline helps to guide technical persons working in computer clubs, cyber-caravans and PIAPs (Public Internet Access Point) located in post offices to set up their infrastructures securely to enable users to access the Internet safely. The guideline also focuses on the precautionary measures required by technical people to manage these facilities.

1.2 Audience

The intended audiences of this document are technical people such as system administrators and IT support officers, working in computer-clubs, post offices and cyber-caravans.

1.3 Document Structure

This document is organised into the following sections:

Section 1 gives an outline of the document's content, the targeted audience and the document's structure.

Section 2 presents a background on Internet access in public places

Section 3 outlines the precautionary measures for configuring Internet securely in Public Places

Section 4 concludes the guideline

2.0 Background

To spread ICT culture and facilitates the emergence of an Information and Knowledge society to reduce the digital divide within the country, the Government is providing broadband Internet access in public places such as post offices and setting up computer-clubs and cyber-caravans. These initiatives will allow citizens to access Information and Communications technologies and to develop their capabilities in social, economic and technological areas.

3.0 Configuring Internet securely in Public Places

Providing Internet access in public places has associated dangers. It is therefore important to take the necessary measures so that users can use the Internet safely.

3.1 System Administration

In computer clubs, post offices or cyber-caravans, it is essential to have an effective and efficient system administration. The System Administrator plays an important role in maintaining the proper functioning and operation of the systems. The following steps can be taken to ensure security:

- The system administrator must ensure that protective measures of the system are functional.
- The responsibilities to create, classify, retrieve, modify, delete or archive information must reset only with the System Administrator
- Any password used for the system administration and operation of trusted services must not be written down or shared with any one.
- A system for password management must be put in place to cover the eventualities such as forgotten password.
- The System Administrator must authorize privileged access to users only on a need-to-know and need-to-do basis.
- The System Administrator together with the system support staff shall conduct regular analysis of problems reported to and identify any weaknesses in protection of the information.

- The operating system and application software should be up to date. Updates are available from vendors on a regular basis. Delete all un-sanctioned programs and directories from the workstations. They can be cleverly renamed as keystroke-capturing programs, network sniffer programs, or viruses.

3.2 Users' Account Management

In order to control access to application systems and data, the following procedures shall be established:

- Users shall be authorized to access the computer services.
- All users shall be required to sign an undertaking to acknowledge that they understand the conditions of access.
- A formal record of all registered users of the computer services shall be maintained.

3.3 Use of applications

Security controls should be installed and maintained on each computer to prevent unauthorized users from gaining entry to the system and prevent any unauthorized access to data. Any system software should only be accessible after being authenticated by access control system (if any).

3.4 System Access Control

Access control shall be implemented to protect the resources and any unauthorized modifications on the operating system. The activities of all users shall be monitored. In addition, an automatic time-out for terminal inactivity should be provisioned if required.

3.5 Use up-to-date anti-virus software

Computer viruses spread easily through portable devices, email, or programs downloaded from the Internet. Potential problems range from changing data to formatting system hard drive. Once created, viruses can spread easily. To protect the systems, it is recommended that a virus scanning/detecting/cleaning program be installed on the computer systems and it should be regularly updated. Set the security software on 'Update Automatically' so that it is kept up-to-date. Configure the anti-virus software properly, so that it actively scans all incoming objects such as removable media for virus infections.

3.6 Maintain anti-virus logs

Anti-virus logs should be maintained for a period of 7-15 days or as determined by the policies of the organization. Ideally a weekly analysis of the logs should be done to obtain an infection profile of viruses and the machines infected.

3.7 Audit Trails & Logs

Audit Trails and log files should be activated as they can be used to record suspicious behaviour. Log files are required for the following:

- To alert for the suspicious activity that requires further investigation.
- To determine the extent of an intruder's activity
- To recover operating system software
- To provide information required for legal proceedings
- To investigate workstation hard disks on a regular basis for suspicious files. Use a naming convention for files and directories. Be sure to look for hidden files and directories.

3.8 Prevention of Computer Misuse

Effective measures to deal with breaches of security shall be established, which include:

- Prompt reporting of suspected breach
- Proper investigation and assessment of the nature of suspected breach
- Secure evidence and preserve integrity of such materials as relates to the discovery of any breach
- Remedial measures
- All the incidents related to breaches shall be reported to the System Administrator for further actions.

4.0 Conclusion

The purpose of providing Internet in public places is to provide the society with computer facilities and Internet access. However, it is the responsibility of the technical person to ensure that the citizens are able to use the facilities properly and securely. For doing so, it is

necessary to take actions that will allow system administrators to observe sign of unexpected behaviours and secure the computer systems accordingly.

5.0 References

- US CERT: http://www.us-cert.gov
- CERT-IN: http://www.cert-in.org.in
- Wikipedia: http://en.wikipedia.org
- CERT-MU: http://www.cert-mu.org.mu