



National Computer Board



CERT-MU

Role of CERT-MU & Future Activities

Mr Vijay Mauree

Manager Planning, Research and Development and CERT-MU

Topics

- Introduction
 - CERT-MU Mission and Objectives
 - CERT-MU Services
 - Local and International Collaboration
 - Incidents
 - Handling intrusions
 - Events and Future Activities
-

Introduction

- CERT-MU launched on 15 May 2008

 - Division of NCB

 - Objectives
 - ◆ Serve as a central point for responding to computer security incidents
 - ◆ Create awareness on security issues through dissemination of information
 - ◆ Increase awareness and understanding of information security and computer security issues
 - ◆ Tracing of latest information on cyber security threats and alerting user community
 - ◆ Publishing whitepapers on computer security aspects including security guidelines
-

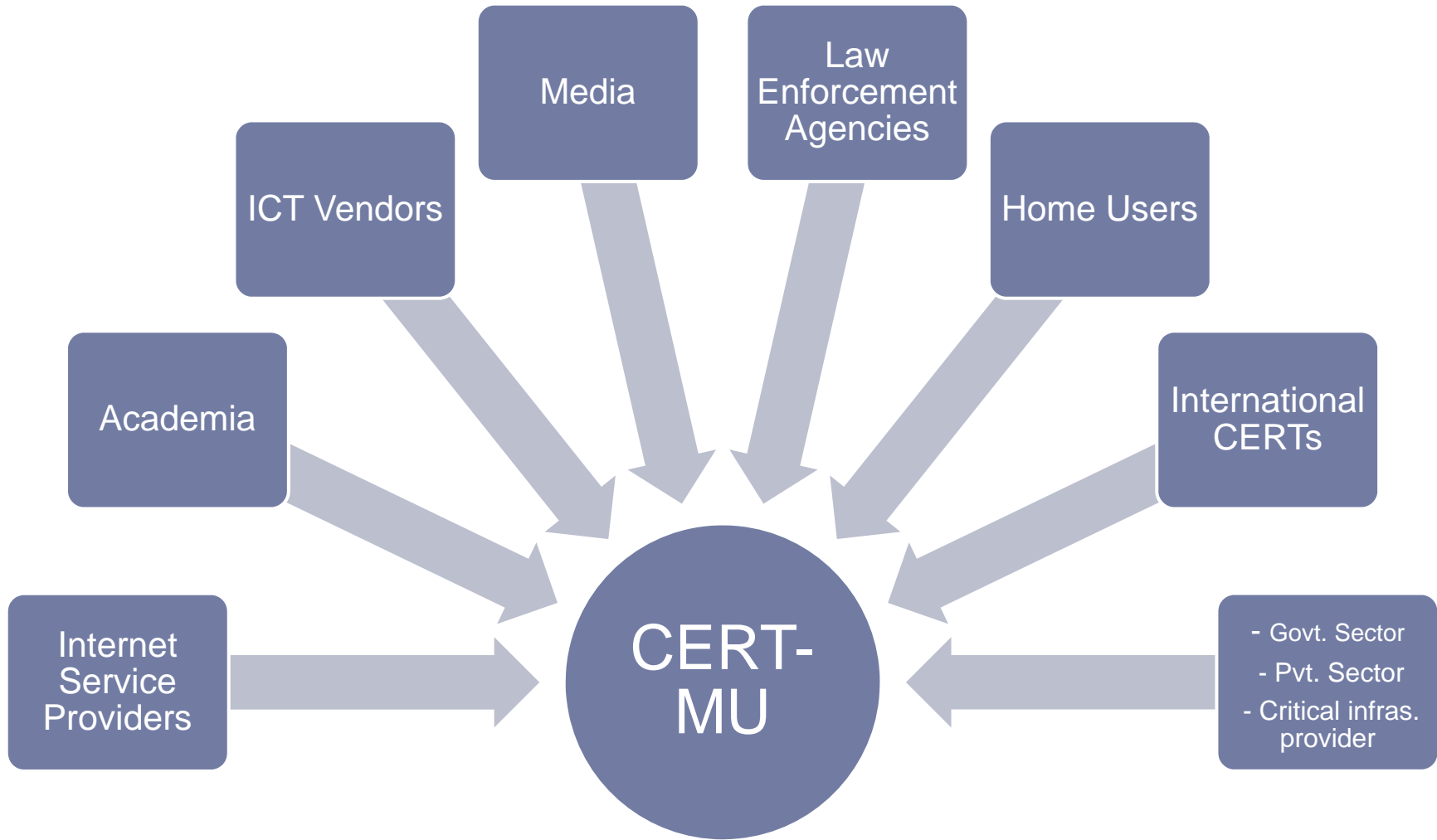
CERT-MU: Mission

To provide information and assistance to its constituents in implementing proactive measures to reduce the risks of information security incidents as well as responding to such incidents as and when they occur.

Aims

- ▶ **Single Point of Contact**
 - ▶ provide a reliable, trusted, single point of contact for prevention, detection & resolution of security incidents on public/private networks such as the Internet in Mauritius
 - ▶ **Increase security competency**
 - ▶ education & awareness promotion
 - ▶ **Provide value-added security services**
 - ▶ security consultancy program
-

CERT-MU: Constituency



CERT-MU Security Services

- ▶ Promote security awareness through the organisation of security seminars and workshops
 - ▶ Responsible for international & industry liaison
 - ▶ Security advisories and alerts online at CERT-MU website
 - ▶ Incident resolution over the phone (office hours) and through email
 - ▶ Technical advice on security issues
 - ▶ Technical assistance to parastatal organisations for ISO 27001
-

Local & International Collaboration

- ▶ CERT-MU works closely with FIRST & international CERTs efforts in the course of its incident response work
 - ▶ Collaboration in area of training and knowledge sharing with foreign CERTs
-

International Contacts

- ▶ CERT-In
 - ▶ Came in May 2008 and CERT-MU Sponsor for FIRST Membership
 - ▶ USCERT
 - ▶ JPCERT/CC (Japan CERT)
 - ▶ UKCERT
 - ▶ MyCERT
-

Reporting an incident

- ▶ Hotline - 800 2378
 - ▶ Web site : <http://cert-mu.org.mu>
 - ▶ Email - incident@cert-mu.gov.mu
 - ▶ Enquiries – info@cert-mu.gov.mu
 - ▶ Incident Report Form
 - ▶ System/Network/Security administrator should be the one reporting the incident
 - ▶ Have information on platform and how you discover the intrusion or break-in
 - ▶ System log files to be made available
-

Incident Resolution

- ▶ Solution may be available immediately if it is a known exploit
 - ▶ If it is some thing new then a work around may be proposed as an interim solution
 - ▶ Confidentiality is maintained at all time
 - ▶ Escalation to law enforcement is the decision of the victim
-

Incidents

- ▶ Typical categories of incidents
 - ▶ Spamming
 - ▶ Denial of Service Attacks
 - ▶ Virus/Trojan Attacks
 - ▶ Email Abuse
-

Handling Intrusions (1)

- ▶ **Prepare**

- ▶ Establish policies and procedures for responding to intrusions

- ▶ **Handle**

- ▶ Analyse all available information to characterise an intrusion
 - ▶ Communicate with all parties that need to be made aware of an intrusion and its progress
-

Handling Intrusions (2)

- ▶ Collect and protect information associated with an intrusion
 - ▶ Apply short-term solutions to contain an intrusion
 - ▶ Eliminate all means of intruder access
 - ▶ Return systems to normal operation with help of incident response team
 - ▶ **Follow up**
 - ▶ Identify and implement security lesson learned
-

CERT-MU Activities

- Workshops on Information Security Issues

October 2008

- Workshop on Adoption of ISO 27001 Information Security Standard
- Workshop on Botnets: Attacks & Defences

December 2008

- Computer Security Day : 2 day conference and capacity building on BS 25999 Business Continuity Planning and Disaster Recovery

February 2009

- Workshop on Privacy & Data Protection

March 2009

- Workshop on Vulnerability Management
-

CERT-MU Future Activities

May 2009

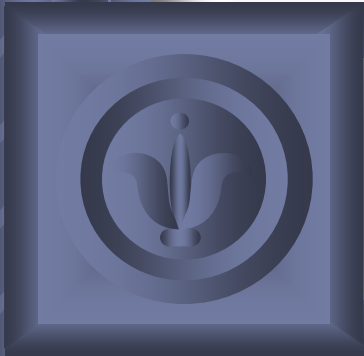
- Capacity Building on ISO 27001
Certified ISMS Implementer's Course
Lead Auditor Course

June 2009

- IPv6 Security Issues
-

CERT-MU Future Activities

- ▶ Protection of Critical Information Infrastructure and National Information Security Assurance
 - ▶ Closer collaboration with constituency
 - ▶ Publication of Information Security Guidelines
 - ▶ Legal framework for Cyber Security
-



Thank You



CERT-MU

<http://www.cert-mu.org.mu>