CERT-MU & Law Enforcement Agencies – Collaboration & Initiatives

CERT-MU

Computer Emergency Response Team of Mauritius

Reechaye Sachindra

Information Security Consultant

National CERT of Mauritius

CERT-MU

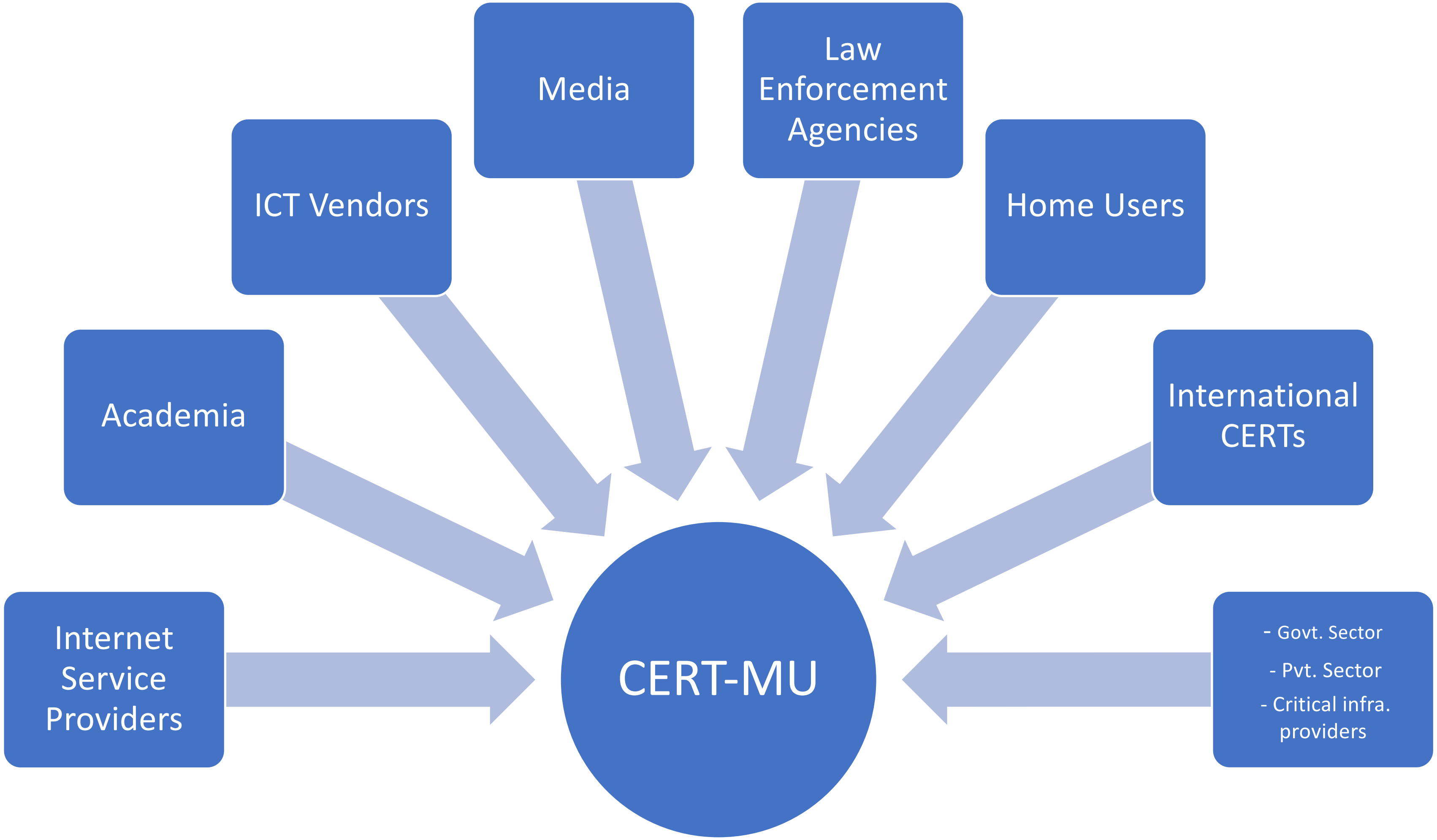
- Key role in preventing cyber-attacks (of criminal nature) and in coordinating response both at national and international level.
- Serve as a central point for reporting and responding to computer security incidents/cybercrimes
- National Advisory Body on Cyber Security issues
- Collaboration with multi-stakeholders including Law Enforcement Agency (LEA) in the fight against cybercrime.

National CERT of Mauritius

- Incident Response and Coordination
- Vulnerability Scanning and Assessment
- Assistance in the Implementation of ISO 27001
- 3rd Party Information Security Audits
- Gap Assessment Exercises-Risk Register-VA/PT
- National Awareness Programme (*Feb 20)
- Child Online Safety Action Plan
- Issuance of Security Alerts (*C19)
- Cyber Exercises
- Capacity Building

CERT-MU

National CERT of Mauritius - Constituency



International Collaboration

- Mauritius is the party to the Commonwealth Cyber Declaration
- Council of Europe’s GLACY, GLACY+
- Council of Europe’s ’s Cyber4D Project (Cyber Resilience Program)
- United Nations Group of Governmental Expert (UNGGE)
- Global Forum on Cyber Expertise (GFCE)
- MoU with Estonia
- MoU with CERT Japan
- Member of FIRST (Forum of Incident Response and Security Teams)
- International CERTs
- ITU (International Telecommunication Union)
- SADC (Southern African Development Community)

Combat against Cybercrime - Stakeholders

- CERT-MU
- Cybercrime Unit
- IT Police Unit
- Internet Service Providers
- Data Protection Office
- Information Communication Technologies Authority
- State Law Office

Social Media - Cyberthreat Enabler

- Phishing
- Scams
- Fake accounts
- Fake news
- Hacked accounts
- Sextortion
- System Compromise
- Identity Theft
- Offensive Content
- Online Harassment

Cyberthreat Landscape: Covid-19 Pandemic (20th March)

Rise in no of scams (26% as compared to 8.6% in February 2020)

- robocalls or mobile phone scams
- lottery scams
- faketortion or Webcam extortion emails
- fake online shops or websites
- charity scams and fraud schemes
- Utilizing the name of Police

Cyberthreat Landscape: Covid-19 Pandemic (20th March)

Misinformation or fake news spread by trolls and fake media

24% of the incidents reported relates to misinformation, as compared to 10% in February 2020.

Unauthorized access over computer systems

represents 19% of the incidents that have been reported as compared to 9% in February 2020.

Initiatives & Collaboration to combat Cybercrime

Monitoring of Cyber Incidents, Analyzing Records, Generating Criminal Justice Statistics

MAUCORS - Mauritian Cybercrime Online Reporting System

(maucors.govmu.org)

- Key initiatives of the National Cybercrime Strategy
- One-stop shop for reporting social media incidents
- Sets out the government’s approach to combat cybercrime in Mauritius.
- Centralized system that connects the Computer Emergency Response Team of Mauritius (CERT-MU), the Cybercrime Unit (Mauritius Police Force), the Data Protection Office and the Information Communication Technologies Authority (ICTA).

Initiatives & Collaboration to combat Cybercrime

- **National Cybersecurity Strategy** - Improve the security and resilience of national infrastructures and services.
- **National Cybercrime Strategy** - Enhancing the Government efforts to tackle cybercrime by providing a more effective law enforcement and criminal justice response
- Developed and Implemented by Ministry of Information Technology, Communication and Innovation (Parent Ministry) & assistance by CERT-MU
- Proposed merger of the two strategies for 2020

Initiatives & Collaboration to combat Cybercrime

National Disaster Cybersecurity and Cybercrime Committee (NDCCC)

- Set-up at the level of Parent Ministry
- Chaired by the Minister of Information Technology, Communication and Innovation
- Monitor and assess the implementation of the action plan set out in the National Cyber Security Strategy and the National Cybercrime Strategy and make recommendations accordingly
- strengthen coordination, collaboration and cooperation relations between the public and private sectors to effectively and efficiently address cyber threats
- Establish areas of cooperation and linkages with regional and international organisations in the area of cybersecurity and cybercrime.
- Advise on the legal framework required to address cybercrime
- Oversee Major Cyber Incidents which can provoke major national ramifications

Initiatives & Collaboration to combat Cybercrime

Some NDCCC Stakeholders

- Ministry of Information Technology, Communication and Innovation
- National CERT
- Law Enforcement Agencies
- Internet Service Providers
- Regulatory Bodies
- Private Sectors

Initiatives & Collaboration to combat Cybercrime

Incident Handling Framework

To clarify roles, responsibilities, authorities and capabilities of stakeholders involved

CERT-MU

- Acts as a focal point to collect and disseminate information to the appropriate audience.
- Activation of Help Desk
- Facilitate information exchange to Ministries, Departments, Public Sector organisations and the Private Sectors
- Advise organisations how to address the problem and facilitate restoration efforts
- Publish advisories

Initiatives & Collaboration to combat Cybercrime

Law Enforcement Agency

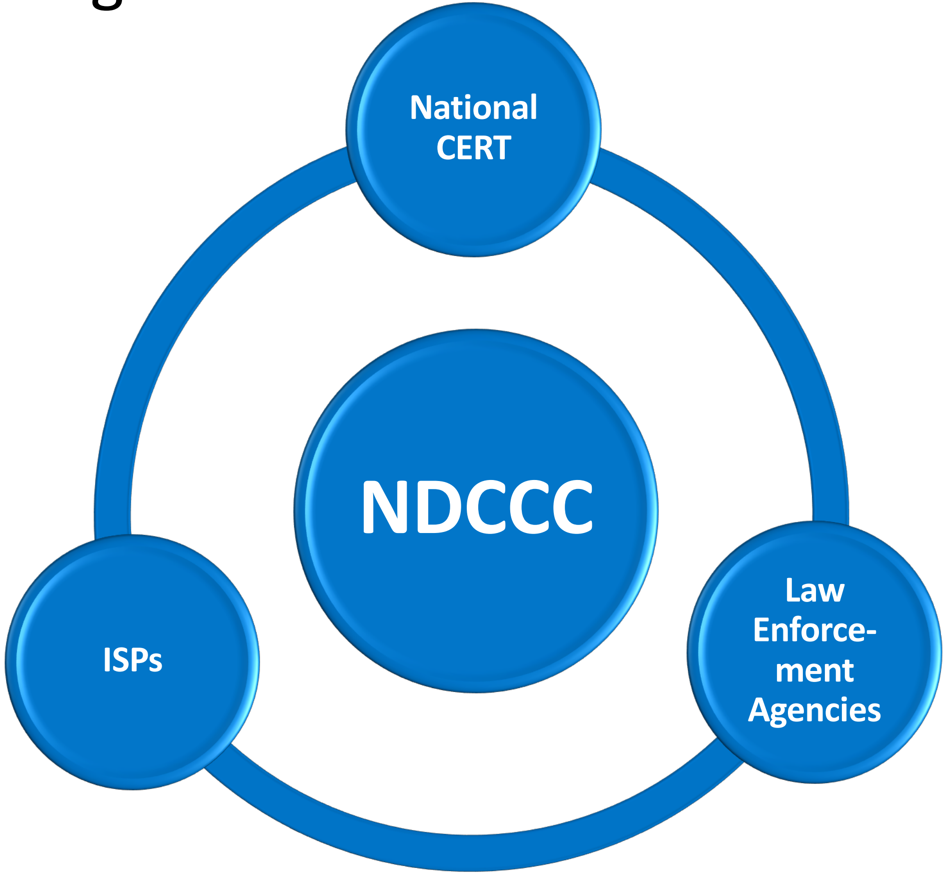
- Gather, preserve and analyse electronic evidence for lega proceedings
- Request technical assistance from CERT-MU
- Present warrants or subpoenas for the disclosure of information.

Internet Service Providers (ISPs)

- Provide information with regards to internet traffic and services in real-time to Law Enforcement
- Information sharing with CERT-MU

Initiatives & Collaboration to combat Cybercrime

Incident Coordinating Team



Initiatives & Collaboration to combat Cybercrime

Capacity Building for Law Enforcement Agencies (LEAs)

Training Programs (Technical, Forensics, Management)

ITU Centre of Excellence –Training Program on Risk Management – LEAs & Regional Countries (CoE - trainings on cybercrime)

Cyber Exercises (Technical and Table-top)

CoE's GLACY, GLACY+

Amendment to local legislations

Cert-MU assisted parent ministry in drafting the amendments of the Computer Misuse and Cybercrime Act for alignment with the Budapest Convention on Cybercrime and with the African Union Convention on Cybersecurity and Personal Data Protection. (COE)

CERT-MU

Initiatives & Collaboration to combat Cybercrime

Projects in the Pipeline

- Development of Critical Infrastructure Protection Policy,
- Setting up of a Cyber Defence Centre
- Accession of AU Convention on Cybersecurity and Personal Data Protection,
- Child online protection capacity building
- Review of Computer Misuse and Cybercrime Act in line with the Budapest Convention on Cybercrime and with the AU Convention on Cybersecurity and Personal Data Protection etc

Enhancements Required

- International Collaboration
- Faster Resolving of Incidents occurring at cross border levels
- Investigations and prosecution of Cybercriminals
- Promote harmonized legislations/adoption of conventions
- Capacity Building of personnel from Judiciary (Prosecutors, Investigators)
- Sharing of Information

Resources Links

CERT-MU Home Page (Vulnerability notes and Information Security News)

http://cert-mu.govmu.org/English/Pages/default.aspx

Cybersecurity Portal

http://cybersecurity.ncb.mu/English/Pages/default.aspx

Information Security Guidelines

http://cert-mu.govmu.org/English/Knowledge%20Bank/Pages/Guidelines.aspx

Online Safety Videos

http://cert-mu.govmu.org/English/Knowledge%20Bank/Pages/Online-Safety-Clips.aspx

E-Security Newsletters by CERT-MU

http://cert-mu.govmu.org/English/Knowledge%20Bank/Pages/e-Security-Newsletter.aspx

THE DATA PROTECTION ACT 2004

http://cert-mu.govmu.org/English/Documents/ICT%20Acts/Data%20Protection%20Act%202004.pdf

THE COMPUTER MISUSE AND CYBERCRIME ACT 2003

http://cert-mu.govmu.org/English/Documents/ICT%20Acts/CMCA%202003.pdf

INFORMATION AND COMMUNICATION TECHNOLOGIES ACT 2001

http://cert-mu.govmu.org/English/Documents/ICT%20Acts/ICT%20Act%202001.pdf

Resources Links (During Covid-19 Pandemic)

Security Alert - Securing a Cybersecurity Workforce

http://cert-mu.govmu.org/English/Documents/Security%20Alerts/2020/March/Security%20alert%20-%20Securing%20a%20Cybersecurity%20Workforce.pdf

Keeping Cyber Healthy during COVID-19 Lockdown Period

http://cert-mu.govmu.org/English/Pages/COVID-19/homepage.aspx

Security Alert on Emotet Security Alert on Phone Scams

http://cert-mu.govmu.org/English/Documents/Security%20Alerts/2020/April/Security%20Alert%20on%20Emotet.pdf

Security Alert on Phone Scams

http://cert-mu.govmu.org/English/Documents/Security%20Alerts/2020/April/Security%20Alert%20on%20Phone%20Scams.pdf

Security Alert on Scams

http://cert-mu.govmu.org/English/Documents/Security%20Alerts/2020/April/Security%20Alert%20on%20Scams.pdf

Security Alert - Fake Email that seems to originate from Mauritius Police Force

http://cert-mu.govmu.org/English/Documents/Security%20Alerts/2020/May/Security%20Alert%20on%20Phishing%20MPF.pdf

Thank You

CONTACT US

Computer Emergency Response Team of Mauritius (CERT-MU)

Tel: 210 55 20 | Hotline: 800 2378

General Enquiry: contact@cert.ncb.mu
Subscribe to Mail List (Security News): subscribe@cert.ncb.mu

MAUCORS: maucors.govmu.org

Incident Reporting: incident@cert.ncb.mu
Vulnerability Reporting: vulnerability@cert.ncb.mu

Website: www.cert-mu.org.mu