Common Market for Eastern and Southern Africa

International Telecommunication Union

ITU Regional Cybersecurity Forum for Eastern and Southern Africa, Lusaka, Zambia, 25-28 August 2008[1]

Document RFL/2008/WG03-E

28 August 2008

Original: English

Working Group 3: Watch, Warning, and Incident Response

Recommendations from the Ad Hoc Forum Working Group on Watch, Warning, and Incident Response

This document aims to provide guidelines and recommendations for the establishment of the necessary national and regional organizational structures to initiate Watch, Warning, and Incident Management activities.

1. Establishment of a National Cybersecurity Center that would serve as national point of contact for Cybersecurity. The Center would constitute the basic building block, to evolve in a more consolidated and structured incident management capability (e.g CERT, CSIRT)

- Related Action:
    a. Development of the action plan according to the guidelines provided in the Annex
- Timing: 1 year (3Q 2009)
- Budget: 100.000 USD per Cybersecurity Center (a more detailed breakdown of costs would be provided later on)

2. Definition and implementation of an awareness campaign, in order to share the national experiences at the regional and international level, involving the relevant organizations including AU, ITU, COMESA, IOC, UNECA, EAC, RIOs etc. The process would lead to obtaining the necessary buy-in from key decision makers and to mobilize the necessary financial and human resources.

- Related Action:
    a. Identification of relevant regional meetings in which the Cybersecurity can be addressed.
    b. Organization of at least an annual international event (at regional or continental level), to review the national activities implemented and build the necessary actions to be implemented at regional and international Level
- Timing: Within 2009 (possibly beginning of 2010). NOTE: The timing would depend on the financial capacity available to initiate national activities. Raising awareness activities would be used for fund raising to establish the National Cybersecurity Center
- Budget: To be defined

3. Establishment of a Regional CERT involving COMESA and any other interested African countries. AU, ITU, COMESA, IOC, UNECA, EAC, RIOs and other international organizations would facilitate the coordination and provide all necessary support to the implementation of the related operational activities. The Regional CERT would link to the National Cybersecurity Centers and would facilitate their evolution to national/government CERT, CSIRT. The implementation of this recommendation would be subsequent to the establishment of the National Cybersecurity Centers.

- Related Action:
    a. ITU, COMESA, UNECA and other interested stakeholders to coordinate and perform the assessment of the operational requirements.
    b. Establishment of the implementation plan

[1] ITU Regional Cybersecurity Forum website: http://www.itu.int/ITU-D/cyb/events/2008/lusaka/

c. Deployment

- Timing: 1 year (4Q 2010, 1Q 2011)
- Budget: To be defined

Annex 1:
Operational Guideline for the Establishment of a National Cybersecurity Center

Critical Success Factors

The guideline aims at providing initial indications, including where possible concrete actions to be taken, on the establishment of a National Cybersecurity Center.

To achieve the expected results, some key critical success factors (CSFs) have to be taken in consideration, and compliancy to these would enable the effective implementation of the concerned activity.

CSFs for the establishment and deployment of a National Cybersecurity Center may include:

- Political Commitment – At the highest level possible
- Awareness – Thorough understanding of the needs and the objectives to be achieved
- Ownership – Clear understanding of concepts such us responsibility and accountability
- Management – Operations, sustainability and business continuity
- Budget – The required financial capacity
- "Start small" approach – To be able to build on existing resources minimizing the initial investment.

Phase 1 – Initial Framework – Establishment of the Security Centre

Objective: Establishment of a full operational cell, able to provide a set of well specified services

Requirements:

Human Resources - (3-4 people):

- IT Engineer – Network/Systems administration
- Security Manager – security measures implementation
- Application specialist - Software solutions deployment
- **Note:** For the initial setup, consideration should be given to appropriate personnel already engaged in government and/or government entities.

Equipment and Facilities:

- Client/Server Configuration (standard server, desktop, etc.)
- LAN
- Printing facilities
- Solid and good broadband internet connectivity - 1MB recommended: Lobby for internet connection sponsorship from local ISP
- Facilities - Physical location etc. Consider autonomous government entities like regulators to house the CERT.

Phase 2 – Scope, Coverage, Roles & Responsibilities

Identify focal point responsible for Cybersecurity

- Specific contact person
- Contingency considerations for focal point contacts
    - Automated e-mail responses for example for confidence assurance purposes
- Services to be provided
    - Simple Incident management
        - Stakeholders incident reporting
        - Data gathering and storing
    - Service support & assistance
        - First level support
    - Capacity Building & Awareness

        - Coordination initiation with the relevant stakeholders (IT Managers, Policy Makers, Regulators, ISPs etc)
        - Website establishment for information sharing
        - Training and workshops
        - Regional awareness campaigns
        - Continental awareness campaigns
- Coverage
    - Government Ministries and Agencies
    - Institutional based type clients – NGOs, Civil Society etc
    - Long term cliental coverage to entire citizenry

Phase 3 - Collaborative Network

- National Coordination
    - ISPs, Data Centers
    - Lobby locally available vendors for sponsorship
    - Mailing lists and contact details for institutional clients
- International coordination
    - Coordination with other IT security centers – CERTS
    - Regional Organizations – COMESA, ITU, UNECA, AU, AFRISPA, EAC, RIOs etc

****