ANNEX 3: GROUPE DE TRAVAIL 3

Common Market for Eastern and Southern Africa

Union internationale des télécommunications

Forum régional UIT sur la cybersécurité pour l'Afrique de l'Est et l'Afrique australe

Lusaka (Zambie), 25-28 août 2008[40]

Doc. RFL/2008/WG02-F

29 août 2008

Original: anglais

Groupe de travail 3: Veille, alerte et intervention en cas d'incident

Recommandations du Groupe de travail ad hoc du Forum sur la veille, l'alerte et l'intervention en cas d'incident

L'objet du présent document est de fournir des lignes directrices et des recommandations relatives à la mise en place des structures organisationnelles nationales et régionales requises pour commencer les activités de veille, d'alerte et de gestion des incidents.

1. Création d'un centre national de cybersécurité qui serait le point de contact national pour la cybersécurité. Ce centre constituerait l'élément de base et évoluerait vers des moyens de gestion des incidents plus complets et plus structurés (par exemple, CERT, CSIRT).

• Activité connexe:

a. Elaboration d'un plan d'action conforme aux lignes directrices figurant à l'Annexe.

• Calendrier: d'ici à un an (troisième trimestre 2009)

• Budget: 100 000 USD par centre de cybersécurité (une ventilation plus détaillée des coûts sera fournie ultérieurement)

2. Elaboration et mise en oeuvre d'une campagne de sensibilisation, afin d'échanger les expériences nationales aux niveaux régional et international, à laquelle participeront les organisations concernées (Union africaine, UIT, COMESA, IOC, CEA, Communauté d'Afrique de l'Est, organisations d'intégration régionale, etc.). Ce processus permettrait d'obtenir l'indispensable adhésion des principaux décideurs et de mobiliser les ressources financières et humaines nécessaires.

• Activités connexes:

a. Identification de réunions régionales dans le cadre desquelles la cybersécurité peut être examinée.

b. Organisation d'au moins une manifestation internationale par an (au niveau régional ou continental) afin de passer en revue les activités nationales en cours et de définir les mesures qu'il est nécessaire de mettre en oeuvre aux niveaux régional et international.

• Calendrier: Courant 2009 (éventuellement début 2010).

• NOTE: Le calendrier dépendrait des ressources financières disponibles pour lancer les activités nationales. Les activités de sensibilisation serviraient à lever des fonds afin de créer le centre national de cybersécurité.

• Budget: A établir.

3. Création d'un CERT régional auquel participerait le COMESA et tout autre pays africain intéressé. L'Union africaine, l'UIT, le COMESA, l'IOC, la CEA, la Communauté d'Afrique de l'Est, des organisations d'intégration régionale et d'autres organisations internationales assureraient la coordination et apporteraient tout l'appui nécessaire à la mise en oeuvre des activités opérationnelles connexes. Le CERT servirait de lien avec les centres nationaux de cybersécurité et faciliteraient leur transformation en CERT

---

40 Site web du Forum régional UIT sur la cybersécurité : http://www.itu.int/ITU-D/cyb/events/2008/lusaka/.

ou CSIRT nationaux/gouvernementaux. La mise en oeuvre de la présente recommandation découlerait de la création de centres nationaux de cybersécurité.

• Activités connexes:

a. Evaluation des besoins opérationnels coordonnée et réalisée par l'UIT, le COMESA, la CEA et d'autres parties prenantes intéressées.

b. Elaboration du plan de mise en oeuvre.

c. Mise en oeuvre.

• Durée: Un an (quatrième trimestre 2010, premier trimestre 2011).

• Budget: A établir.

Annexe 1 :

Lignes directrices opérationnelles relatives à la création d'un centre national de cybersécurité

Facteurs clés de réussite

L'objet des présentes lignes directrices est de donner des orientations de départ, y compris d'indiquer les domaines dans lesquels des mesures concrètes peuvent être prises, concernant la création d'un centre national de cybersécurité.

Pour obtenir les résultats escomptés, il faut tenir compte de certains facteurs clés de réussite, dont le respect permettrait de mettre en oeuvre efficacement l'activité en question.

Ces facteurs indispensables à la création et à la mise en oeuvre d'un centre national de cybersécurité seront peut-être les suivants:

• Volonté politique: au plus haut niveau possible.

• Connaissance: compréhension approfondie des besoins et des objectifs à atteindre.

• Structure: définition claire des concepts comme la responsabilité individuelle et administrative.

• Gestion: fonctionnement, viabilité et durabilité.

• Budget: capacité financière requise.

• Développement progressif: possibilité d'utiliser les ressources existantes afin de minimiser l'investissement de départ.

Phase 1 – Cadre initial - Création d'un centre de sécurité

Objectif: Création d'une cellule opérationnelle complète capable de fournir un ensemble de services bien définis.

Besoins:

Ressources humaines (3-4 personnes):

• Ingénieur en technologies de l'information - Administration de réseaux/systèmes.

• Responsable de la sécurité - Mise en oeuvre des mesures de sécurité.

• Spécialiste d'applications - Déploiement de solutions logicielles.

• NOTE : Pour la structure de départ, il conviendrait d'envisager d'avoir recours au personnel adéquat dont disposent déjà les pouvoirs et/ou les organismes publics.

Equipements et installation:

• Configuration client/serveur (serveur standard, bureau, etc.).

• Réseau local.

• Imprimantes.

• Connexion Internet large bande solide et efficace - 1 Mb recommandé: faire du lobbying auprès de fournisseurs de services Internet locaux pour obtenir une connexion Internet gratuite.

• Installations: emplacement physique, etc. Envisager la possibilité que des entités publiques autonomes, comme les régulateurs, hébergent le CERT.

Phase 2 – Compétences, bénéficiaires, rôles et responsabilités

Identifier un coordonnateur chargé de la cybersécurité.

• Interlocuteur spécifique.

• Eventualités devant être prises en compte par le coordonnateur:

  - Accusés de réception automatiques par courrier électronique, par exemple, pour rassurer l'utilisateur.

• Services à fournir:

  – Gestion d'incidents simples:

- Signaler les incidents aux parties prenantes.
- Recueillir et stocker des données.

– Appui aux services et assistance:

- Premier niveau d'appui.

– Renforcement des capacités et sensibilisation:

- Assurer la coordination avec les parties prenantes concernées (responsables en matière de technologies de l'information, décideurs, régulateurs, fournisseurs de services Internet, etc.).
- Créer un site web permettant d'échanger des informations.
- Organiser des formations et des ateliers.
- Mener des campagnes de sensibilisation à l'échelle de la région.
- Mener des campagnes de sensibilisation à l'échelle du continent.

• Bénéficiaires:

– Ministères et organismes publics.

– Clients institutionnels (ONG, société civile, etc.).

– A long terme, tous les citoyens.

Phase 3 – Réseau de collaboration

• Coordination nationale:

– Fournisseurs de services Internet, centres de données.

– Sollicitation des fournisseurs de services locaux afin d'obtenir un sponsoring.

– Listes de diffusion et coordonnées des clients institutionnels.

• Coordination internationale:

– Coordination avec d'autres centres de sécurité dans le domaine des technologies de l'information - CERT.

– Organisations régionales (COMESA, UIT, CEA, Union africaine, AFRISPA, Communauté d'Afrique de l'Est, organisations d'intégration régionale, etc.).

_____