UNION INTERNATIONALE DES TÉLÉCOMMUNICATIONS

BUREAU DE DÉVELOPPEMENT DES TÉLÉCOMMUNICATIONS

Document 14-F
13 décembre 2007
Original: anglais

6ÈME REUNION SUR LES INDICATEURS DES TELECOMMUNICATIONS/TIC DANS LE MONDE, GENEVE, 13-15 DÉCEMBRE 2007

ORIGINE: UIT/BDT

TITRE: Evaluer l'état de préparation des pays en matière de cybersécurité

_____

Evaluer l'état de préparation des pays en matière de cybersécurité

Réunion sur les indicateurs des télécommunications/TIC dans le monde, Genève (Suisse)

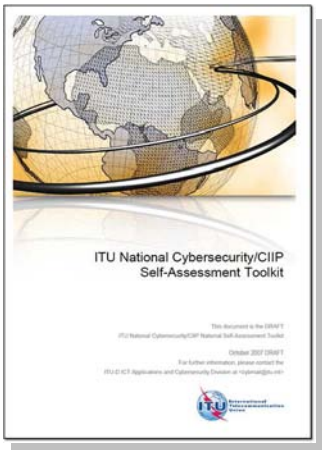
13-15 décembre 2007

Robert Shaw
<robert.shaw@itu.int>
Chef, Division applications TIC et cybersécurité
www.itu.int/ITU-D/cyb
Département des politiques et stratégies
Secteur du développement des télécommunications de l'UIT (UIT-D)

Le contexte

- Le XXIe siècle est caractérisé par une dépendance croissante vis-à-vis des technologies de l'information et de la communication (TIC), universellement répandues;
- La croissance rapide des TIC et cette dépendance ont modifié depuis une douzaine d'années la perception des menaces planant sur la cybersécurité;
- Interdépendance croissante entre la cybersécurité et la protection des infrastructures essentielles de l'information (CIIP);
- Plusieurs pays ont commencé à évaluer leurs points faibles et les risques et ont réfléchi aux moyens d'y faire face;
- Néanmoins, la plupart d'entre eux n'ont pas encore formulé ou mis en oeuvre de stratégie nationale de cybersécurité ou de programme de protection des infrastructures essentielles de l'information (CIIP);
- La nécessité de traiter le problème au niveau national se fait de plus en plus sentir:
  - Dans ce contexte, comment évaluer la situation des différents pays?

Aperçu des activités en rapport avec le Secteur du développement de l'UIT (UIT-D)



- Question 22/1 de la Commission d'études 1 du Secteur du développement de l'UIT – Meilleures pratiques recommandées pour parvenir à la cybersécurité
- Activités menées dans le cadre des efforts pour assurer la cybersécurité/la protection des infrastructures essentielles de l'information au niveau national
- Module UIT d'auto-évaluation sur la cybersécurité et la protection des infrastructures essentielles de l'information au niveau national

Cadre général des efforts nationaux en matière de cybersécurité	Elaborer des stratégies nationales	Favoriser la collaboration entre secteur public et secteur privé	Prévenir la cybercriminalité	Créer des dispositifs de gestion des incidents	Promouvoir une culture de la cybersécurité
Politiques	Politiques visant à guider les efforts déployés par les pays				
Objectifs	Objectifs visant à mettre en oeuvre les politiques				
Mesures à prendre	Mesures visant à atteindre ces objectifs				
Ressources	Ressources à l'appui des efforts déployés par les pays				

Initiatives de l'UIT

- Moyens utilisés par l'UIT à l'appui du cadre général et des mesures de mise en oeuvre sur le plan national:
  - Documents de référence et ressources en matière de formation
    - http://www.itu.int/ITU-D/cyb/cybersecurity/
  - Module UIT d'auto-évaluation sur la cybersécurité et la protection des infrastructures essentielles de l'information au niveau national
    - www.itu.int/ITU-D/cyb/cybersecurity/projects/readiness.html
  - Réunions régionales sur les cadres applicables à la cybersécurité et à la protection des infrastructures essentielles de l'information
    - http://www.itu.int/ITU-D/cyb/events/

Réunions régionales UIT sur les cadres applicables à la cybersécurité/CIIP

- 2007
  - Hanoi (Viet Nam)
  - Buenos Aires (Argentine)
  - Praia (Cap-Vert)
- 2008
  - Oman (Qatar)
  - Indonésie
  - Amérique latine et Caraïbes
  - Bulgarie
  - Afrique

A ce jour,

- Plusieurs pays ont manifesté leur intérêt pour l'établissement d'un indice national sur l'état de préparation à la cybersécurité, outil qui permettrait:
  - de sensibiliser à la nécessité d'élaborer une politique nationale
  - d'établir une évaluation comparative de l'état d'avancement de la mise en oeuvre d'un cadre général dans différents pays
    - Où en est-on?

Problèmes qui se posent aux spécialistes des indicateurs

- Comment établir un indice par rapport aux éléments d'un cadre?
- Certains de ces éléments sont très difficiles à mesurer:
  - Stratégie nationale
  - Collaboration secteur public – secteur privé
  - Prévention de la cybercriminalité
  - Création, au niveau national, d'un dispositif de gestion des incidents
  - Promouvoir une culture de la cybersécurité

Activités à prendre en compte pour l'établissement d'un tel indice

- Etude exploratoire de l'OCDE pour la mesure de la confiance dans l'environnement en ligne
  - http://www.oecd.org/dataoecd/26/15/35792806.pdf
- Activités de la Korea Information Security Agency
  - Elaboration d'un indice national de la sécurité de l'information
- Conformité des législations nationales aux articles de fond et de procédure de la Convention de Budapest sur la cybercriminalité (2001)
- Travaux CERT CSIRT sur la mesure des capacités de gestion des incidents
  - http://www.cert.org/csirts/metrics.html
- Forum for Incident Response and Security Teams (FIRST)
  Equipes CSIRT – Prescription de constatation?
- Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA)
  - Collecte de données sur les incidents relatifs à la sécurité et à la confiance des consommateurs:
    http://www.enisa.europa.eu/pages/data_collection/

Union
internationale
des télécommunications

Aider le monde à communiquer