Bureau de développement des télécommunications (BDT)

Réf.: BDT/POL/CYB/Circular-002

Genève, le 15 février 2011

Etats Membres

Contact: Souheil Marine
Téléphone: +41 22 730 6057
Télécopie: +41 22 730 5484
E-mail: cybersecurity@itu.int

Sujet: Partenariat UIT-IMPACT – Déploiement de capacités dans le domaine de la cybersécurité

Madame, Monsieur,

Je vous écris en ma qualité de nouveau Directeur du Bureau de développement des télécommunications de l'UIT (BDT) pour informer votre Administration que le BDT continuera à soutenir le Partenariat multilatéral international contre les cybermenaces (IMPACT) et s'engage à continuer d'aider les Etats Membres à renforcer la confiance et la sécurité pour ce qui est de l'utilisation des TIC.

Comme vous le savez, l'UIT et IMPACT ont officiellement conclu en 2008 un Mémorandum d'accord aux termes duquel le nouveau siège ultramoderne d'IMPACT situé à Cyberjaya (Malaisie) est devenu le siège et l'agent d'exécution du Programme mondial cybersécurité (GCA) de l'UIT.

Les synergies étroites établies entre les cinq grands axes du Programme GCA et les services et infrastructures fournis par IMPACT font de ce partenariat une étape décisive dans la lutte mondiale contre les cybermenaces et autres utilisations abusives des TIC, en même temps qu'elles aident les Etats Membres à renforcer leurs capacités dans le domaine de la cybersécurité.

En tant que Directeur du BDT, je suis déterminé à tirer parti des succès obtenus et à mettre en œuvre de nouvelles initiatives et de nouveaux projets conformes aux résolutions de la CMDT-10 et de la PP-10.

L'UIT, par l'intermédiaire de ses Secteurs, en particulier du BDT, a acquis une expérience certaine en matière d'assistance à l'élaboration de stratégies nationales pour la cybersécurité et la protection des infrastructures essentielles de l'information et peut compter sur l'appui d'un vaste réseau d'organismes et de particuliers faisant référence dans le domaine de la cybersécurité.

Conformément aux cinq grands axes du Programme GCA, ainsi que pour donner suite aux activités menées par l'UIT pour aider les pays à développer des capacités en matière de cybersécurité, le partenariat UIT-IMPACT met à la disposition des Etats Membres ses compétences spécialisées pour leur permettre de détecter et d'analyser les cybermenaces et d'y faire face.

Le Centre d'alerte mondial (GRC) est une plate-forme mondiale de systèmes d'alerte avancée et la principale ressource dont dispose la communauté internationale dans la lutte contre les cybermenaces; à ce titre, il assure des services d'intervention d'urgence et propose des moyens de partage du savoir dans un environnement sécurisé.

La plate-forme électronique sécurisée d'applications collaboratives pour les experts ESCAPE fait partie intégrante des services liés au GRC et fournis par le partenariat ITU-IMPACT aux Etats Membres. Cet outil permet aux experts de la cybersécurité dans différents pays de mettre en commun leurs ressources, d'échanger des compétences techniques et de collaborer à distance, dans un environnement sécurisé. Grâce à la plate-forme ESCAPE, le GRC peut constituer en quelque sorte un pôle unique de coordination et d'intervention en situation de crise, permettant aux pays d'identifier et de mettre en commun rapidement les ressources existantes et les moyens de gestion des incidents et d'intervention en cas d'incident. Quelque 70 Etats Membres sont aujourd'hui membres du partenariat UIT-IMPACT et bénéficient des services du GRC, gratuitement.

En outre, les Etats Membres qui deviennent membres du partenariat UIT-IMPACT peuvent demander à bénéficier de formations et de bourses d'études fournies par IMPACT et par des partenaires tels que le SANS Institute, le EC Council, l'ISC^2, etc.

Par ailleurs, il faut mettre en place sur le plan national des structures spécialisées chargées de faire face aux cyberattaques. Dans cette optique, le partenariat UIT-IMPACT a élaboré une stratégie de mise en œuvre d'équipes nationales d'intervention en cas d'incident informatique (CIRT) - points de contact centralisés et sécurisés de coordination de la cybersécurité dans un pays - chargées d'assurer des fonctions de veille et d'alerte et d'intervenir en cas d'incident. La démarche ainsi proposée serait intégrée dans les services déjà fournis par le GRC et serait conforme aux bonnes pratiques internationales.

Le partenariat UIT-IMPACT a déjà mené à bien une évaluation pour 21 pays et prévoit de poursuivre cette activité en facilitant la mise en œuvre matérielle des équipes CIRT, par la fourniture des compétences spécialisées nécessaires en vue de recommander les matériels et logiciels les plus adaptés, l'assistance à l'élaboration des processus requis et le renforcement des capacités humaines.

Vous trouverez dans les annexes à la présente lettre un aperçu des services actuellement proposés, ainsi que les documents nécessaires pour devenir membre du partenariat UIT-IMPACT (lettre-réponse type et profil de pays, à remplir). Vous trouverez en ligne de plus amples informations sur IMPACT à l'adresse:

- http://www.itu.int/ITU-D/cyb/cybersecurity/impact.html

Si votre pays n'est pas déjà membre du partenariat UIT-IMPACT, et souhaite participer aux activités mentionnées plus haut, nous vous invitons à répondre à la présente lettre en signalant le domaine et les services précis auxquels votre pays s'intéresse.

Nous vous souhaitons la bienvenue parmi nous et comptons recevoir de votre part des contributions utiles qui nous permettront de mieux prêter assistance aux Etats Membres de l'UIT.

Je vous prie d'agréer, Madame, Monsieur, l'expression de ma haute considération.

[Original signée]

Brahima Sanou
Directeur

Annexes:

- Notes techniques:
  - Centre d'alerte mondial (GRC)
  - Centre IMPACT de formation et de renforcement des compétences
- Lettre-réponse type
- Formulaire "profil de pays"

CC: Directeurs des Bureaux régionaux de l'UIT