|  |  |  |
| --- | --- | --- |
|  | Assemblée mondiale de normalisation des télécommunications (AMNT-24)New Delhi, 15-24 octobre 2024 |  |
|  |
|  |  |
| SÉANCE PLÉNIÈRE | Addendum 10 auDocument 35-F |
|  | 13 septembre 2024 |
|  | Original: anglais |
|  |
| Administrations des pays membres de l'Union africainedes télécommunications |
| PROPOSition de MODIFICATION de la RéSOLUTION 58 |
|  |
|  |

|  |  |
| --- | --- |
| **Résumé:** | Dans la présente contribution, il est proposé d'actualiser la Résolution 58 de l'Assemblée mondiale de normalisation des télécommunications pour demander aux États Membres d'aider les équipes d'intervention en cas d'incident informatique à améliorer les échanges d'informations et la collaboration aux fins des interventions en cas d'incident de cybersécurité, en particulier dans les pays en développement partout dans le monde. Les États Membres sont appelés à élaborer et mettre en œuvre des programmes de sensibilisation sur l'importance des équipes d'intervention en cas d'incident informatique. |
| **Contact:** | Isaac BoatengUnion africaine des télécommunications | Courriel: i.boateng@atuuat.africa |

Introduction

L'objectif est d'aider les équipes d'intervention en cas d'incident informatique (CIRT) à intensifier les échanges d'informations et la collaboration aux fins des interventions en cas d’incident de cybersécurité, en particulier dans les pays en développement, ce qui aura pour effet d'améliorer la préparation aux situations d'urgence liées à la cybersécurité et de rendre le dispositif de cybersécurité plus fort et plus résilient, en particulier dans ces pays.

MOD ATU/35A10/1

RÉSOLUTION 58 (Rév. New Delhi, 2024)

Encourager la création d'équipes nationales d'intervention en cas d'incident informatique, en particulier pour les pays en développement

(Johannesburg, 2008; Dubaï, 2012; Genève, 2022; New Delhi, 2024)

L'Assemblée mondiale de normalisation des télécommunications (New Delhi, 2024),

considérant

que par sa Résolution 123 (Rév. Bucarest, 2022), la Conférence de plénipotentiaires a chargé le Secrétaire général et les Directeurs des trois Bureaux d'œuvrer en étroite coopération à la mise en œuvre d'initiatives permettant de réduire l'écart qui existe en matière de normalisation entre pays en développement et pays développés,

considérant en outre

que la Recommandation UIT-T X.1060 fournit un cadre relatif à la création et à l'exploitation d'un centre de cyberdéfense,

reconnaissant

*a)* les résultats très satisfaisants obtenus par l'approche régionale dans le cadre de la Résolution 54 (Rév. Hammamet, 2016) de l'Assemblée mondiale de normalisation des télécommunications;

*b)* que les pays en développement utilisent de plus en plus d'ordinateurs et sont de plus en plus tributaires des ordinateurs pour les technologies de l'information et de la communication (TIC);

*c)* les attaques et menaces de plus en plus nombreuses ciblant les réseaux TIC par l'intermédiaire d'ordinateurs;

*d)* les travaux menés par le Secteur du développement des télécommunications de l'UIT (UIT‑D) dans le cadre de l'ancienne Question 22/1 de la Commission d'études 1 de l'UIT-D et l'actuelle Question 3/2 de la Commission d'études 2 de l'UIT-D sur ce sujet,

notant

*a)* que le niveau de préparation aux situations d'urgence informatique est encore peu élevé dans de nombreux pays, en particulier dans les pays en développement;

*b)* que le degré élevé d'interconnectivité des réseaux TIC pourrait être affecté en cas d'attaque lancée depuis des réseaux des pays les moins bien préparés, qui sont pour la plupart des pays en développement;

*c)* qu'il est important d'avoir un niveau approprié de préparation aux situations d'urgence informatique dans tous les pays;

*d)* qu'il est nécessaire de créer des équipes d'intervention en cas d'incident informatique (CIRT) à l'échelle nationale et qu'il est important d'assurer une coordination à l'intérieur des régions et entre les régions;

*e)* les travaux menés par la Commission d'études 17 du Secteur de la normalisation des télécommunications de l'UIT (UIT-T) concernant les équipes CIRT, en particulier pour les pays en développement, et la coopération entre ces équipes, comme indiqué dans les documents établis par cette commission d'études;

*f)* qu'il est de plus en plus complexe de gérer les infrastructures, outils et effectifs de cyberdéfense et les services de sécurité connexes étant donné la sophistication croissante des cyberattaques dont les réseaux TIC font l'objet dans tous les pays,

ayant à l'esprit

que des équipes CIRT qui fonctionnent bien dans les pays en développement permettront d'améliorer le niveau de participation de ces pays aux activités mondiales d'intervention en cas d'urgence informatique et de contribuer à obtenir une infrastructure TIC efficace et une expertise en matière de cybersécurité à l'échelle mondiale,

décide

1 d'appuyer la création d'équipes CIRT nationales dans les États Membres où de telles équipes sont nécessaires et n'existent pas actuellement;

2 d'aider les équipes CIRT à améliorer les échanges d'informations et la collaboration aux fins des interventions en cas d'incident de cybersécurité, afin d'accroître le niveau de préparation aux situations d'urgence liées à la cybersécurité, en particulier dans les pays en développement partout dans le monde;

3 d'associer les bureaux régionaux de l'UIT pour ce qui est de mettre en œuvre la présente Résolution et de mieux faire connaître l'importance des équipes CIRT pour les États Membres et sur les activités menées par l'UIT-T sur cette question,

charge le Directeur du Bureau de la normalisation des télécommunications

de rendre compte chaque année au Groupe consultatif de la normalisation des télécommunications de la mise en œuvre de la présente Résolution,

charge le Directeur du Bureau de la normalisation des télécommunications, en collaboration avec le Directeur du Bureau de développement des télécommunications

1 de définir de bonnes pratiques pour l'établissement d'équipes CIRT conformément au kit pratique de l'UIT;

2 de déterminer là où des équipes CIRT nationales sont nécessaires, en particulier dans les pays en développement, et d'encourager la création de ces équipes;

3 de collaborer avec des experts et des organismes internationaux pour l'établissement d'équipes CIRT nationales;

4 de fournir un appui, selon les besoins et dans les limites des ressources budgétaires existantes;

5 de faciliter la collaboration entre les équipes CIRT nationales, par exemple en matière de renforcement des capacités et d'échange d'informations, dans un cadre adapté;

6 de prendre les mesures nécessaires pour promouvoir la mise en œuvre de la présente Résolution;

7 d'élaborer des programmes de sensibilisation sur l'importance des équipes CIRT pour ce qui est d'accroître le niveau du dispositif de cybersécurité,

invite les États Membres

1 à envisager la création, à titre hautement prioritaire, d'une équipe CIRT nationale;

2 à collaborer avec les autres États Membres et avec les Membres de Secteur;

3 à encourager la création de réseaux de collaboration et la participation aux initiatives des organisations internationales telles le Forum des équipes d'intervention et de sécurité en cas d'incident (FIRST) pour renforcer, à l'échelle mondiale, les capacités en matière de cybersécurité et la collaboration aux fins des interventions en cas d'incident,

invite les États Membres et les Membres de Secteur

à coopérer étroitement avec l'UIT-T, l'UIT-D et les bureaux régionaux de l'UIT en la matière.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_