|  |  |  |  |
| --- | --- | --- | --- |
|  | Assemblée mondiale de normalisation des télécommunications (AMNT-24) New Delhi, 15-24 octobre 2024 | |  |
|  | | | |
|  | |  | |
| SÉANCE PLÉNIÈRE | | Addendum 13 au Document 37-F | |
|  | | 22 septembre 2024 | |
|  | | Original: anglais | |
|  | | | |
| Administrations des pays membres de la Télécommunauté Asie-Pacifique | | | |
| PROPOSITION DE MODIFICATION DE LA RÉSOLUTION 58 | | | |
|  | | | |
|  | | | |

|  |  |  |
| --- | --- | --- |
| **Résumé:** | Étant donné que les cybermenaces et les cyberattaques contre les infrastructures mondiales de télécommunication/TIC ne cessent de croître et d'évoluer, il est nécessaire de prévoir un niveau approprié d'intervention en cas d'urgence liée à la cybersécurité dans tous les pays; en outre le rôle des équipes d'intervention en cas d'incident informatique (CIRT) est plus essentiel que jamais. Dans le présent document, il est proposé d'apporter des modifications à la Résolution 58 de l'AMNT. | |
| **Contact:** | M. Masanori Kondo Secrétaire général Télécommunauté Asie-Pacifique | Courriel: [aptwtsa@apt.int](mailto:aptwtsa@apt.int) |

Introduction

Alors que les services et les technologies liés aux infrastructures de télécommunication/TIC continuent d'évoluer, les cybermenaces et les cyberattaques évoluent elles aussi. Les cybermenaces peuvent se diffuser non seulement par les ordinateurs, mais aussi par les dispositifs mobiles, les serveurs, les réseaux et même les technologies opérationnelles. Par ailleurs, les cyberattaques ciblent de plus en plus les infrastructures de télécommunication/TIC essentielles et les données importantes.

Compte tenu de l'augmentation rapide du volume, de la gravité et de la sophistication des cybermenaces et des cyberattaques, la sécurité reste une préoccupation mondiale et il est nécessaire d'aider les pays, en particulier les pays en développement, à protéger leurs réseaux de télécommunication/TIC contre les cybermenaces et les cyberattaques. Le rôle des équipes d'intervention en cas d'incident informatique (CIRT) est essentiel pour intervenir en cas d'incident de manière appropriée et devrait être renforcé. Cependant, le niveau de préparation aux incidents de cybersécurité reste faible dans de nombreux pays, en particulier dans les pays en développement. Il est donc important de créer des équipes CIRT au niveau national et de renforcer l'échange d'informations et la collaboration entre les gouvernements et les autres parties prenantes en matière d'intervention en cas d'incident de cybersécurité. L'élaboration de Recommandations et de Suppléments peut faciliter la création d'équipes CIRT et la promotion d'un cadre opérationnel pour les équipes CIRT, comme c'est le cas de la Recommandation UIT-T X.1060, intitulée "Cadre relatif à la création et à l'exploitation d'un centre de cyberdéfense", qui donne des lignes directrices sur la manière de veiller à ce que les organisations soient préparées au moyen de capacités de cyberdéfense et de services de sécurité efficaces, y compris les interventions en cas d'incident de cybersécurité.

L'AMNT-20 a mis à jour la Résolution 58, qui traite de la nécessité urgente de créer des équipes CIRT nationales dans tous les pays, en mettant l'accent sur la réduction de l'écart en matière de cybersécurité entre les pays en développement et les pays développés. Cette Résolution vise à tenir compte de la mise à jour de la Résolution 130 (Rév. Bucarest, 2022) de la Conférence de plénipotentiaires en ce qui concerne la promotion du cadre opérationnel pour les équipes CIRT.

L'objectif principal de la modification de la Résolution 58 proposée est de contribuer à améliorer les niveaux d'intervention en cas d'urgence liée à la cybersécurité dans le monde.

Proposition

Les Administrations des pays membres de la Télécommunauté Asie-Pacifique proposent de réviser la Résolution 58 de l'AMNT.

MOD APT/37A13/1

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[[1]](#footnote-1)1

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

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

considérant

*a)* la Résolution 130 (Rév. Bucarest, 2022) de la Conférence de plénipotentiaires sur le renforcement du rôle de l'UIT dans l'instauration de la confiance et de la sécurité dans l'utilisation des technologies de l'information et de la communication (TIC);

*b)* que par sa Résolution 123 (Rév. Dubaï, 2018), 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)* les travaux bénéficiant d'un rang de priorité élevé et concernant la Résolution 50 (Rév. New Delhi, 2024), menés à l'UIT-T conformément à ses compétences et à ses connaissances spécialisées, notamment en favorisant une compréhension commune, entre les gouvernements et les autres parties prenantes, de l'instauration de la confiance et de la sécurité dans l'utilisation des TIC aux niveaux national, régional et international;

*c)* le niveau croissant de la transformation numérique des pays en développement et leur dépendance croissante vis-à-vis des technologies de l'information et de la communication (TIC);

*d)* l'augmentation rapide du volume, de la gravité et du degré de sophistication des cybermenaces et des cyberattaques contre les infrastructures de télécommunication/TIC et la complexité de la gestion des infrastructures, des outils, des personnes et des services de sécurité relatifs à la cyberdéfense;

*e)* qu'en raison de l'évolution constante des services et des technologies liés aux infrastructures de télécommunication/TIC, les cybermenaces et les cyberattaques évoluent elles aussi, que les cybermenaces peuvent se diffuser non seulement par les ordinateurs, mais aussi par les dispositifs mobiles, les serveurs, les réseaux et même les technologies opérationnelles, tandis que les cyberattaques ciblent de plus en plus les infrastructures de télécommunication/TIC essentielles et les données importantes;

*f)* 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 liées à la cybersécurité 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 et régions les moins bien préparés;

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

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

*e)* qu'il existe plusieurs synonymes pour les équipes CIRT (équipes d'intervention en cas d'incident informatique/équipes d'intervention en cas d'incident de cybersécurité): CERT (équipe d'intervention en cas d'urgence informatique), équipes de réponse aux incidents de sécurité informatique (CSIRT), CIRC (centre d'intervention en cas d'incident informatique) ou CDC (centre de cyberdéfense);

*f)* 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, par exemple la Recommandation UIT-T X.1060, intitulée "Cadre relatif à la création et à l'exploitation d'un centre de cyberdéfense", pour faire en sorte que les organisations soient préparées au moyen de capacités de cyberdéfense et de services de sécurité efficaces pour se protéger contre les cyberattaques et les menaces de sécurité,

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 liée à la cybersécurité et de contribuer à obtenir une infrastructure mondiale TIC efficace et sûre,

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 et de promouvoir le cadre opérationnel connexe des équipes CIRT dans les États Membres où de telles équipes sont mises en place, le cas échéant;

2 d'aider le Directeur du BDT à promouvoir les bonnes pratiques nationales, régionales et internationales relatives à la mise en place d'équipes CIRT, en fournissant des Recommandations techniques et des Suppléments,

charge la Commission d'études 17

1 de continuer à élaborer des Recommandations et des Suppléments qui facilitent la création d'équipes CIRT et de promouvoir un cadre opérationnel pour ces équipes;

2 d'encourager les études concernant le cadre relatif aux centres de cyberdéfense, qui vise à réduire au minimum les cyberrisques et les incidences des failles de sécurité grâce à des processus et des procédures de détection et d'intervention efficaces ainsi qu'à des technologies et des méthodes d'évaluation des services de sécurité pour les infrastructures de télécommunication/TIC mondiales;

3 d'appuyer le Directeur du Bureau de la normalisation des télécommunications dans les initiatives visant à réduire l'écart en matière de normalisation entre les pays en développement et les pays développés en ce qui concerne les CDC, qui devraient comprendre des sujets d'étude sur les travaux de normalisation des CDC liés à la sécurité, et de les partager avec les groupes concernés de l'UIT-D dans le cadre de sa mission de commission d'études directrice pour la sécurité;

4 de promouvoir les activités conjointes de coordination sur les CDC entre toutes les commissions d'études et tous les groupes spécialisés concernés de l'UIT, ainsi qu'avec d'autres organisations de normalisation;

5 de continuer de définir un ensemble de capacités des CDC, y compris l'infrastructure et l'organisation, ainsi que d'appliquer l'approche de la sécurité dès la conception aux CDC (c'est‑à‑dire d'appliquer les capacités et les fonctionnalités de sécurité disponibles dès la phase de conception) pour les infrastructures de télécommunication/TIC,

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 et de promouvoir le cadre opérationnel connexe, 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,

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,

invite les États Membres et les Membres de Secteur

à coopérer étroitement avec l'UIT-T et l'UIT-D en la matière.

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

1. 1 Les pays en développement comprennent aussi les pays les moins avancés, les petits États insulaires en développement, les pays en développement sans littoral et les pays dont l'économie est en transition. [↑](#footnote-ref-1)