Bureau de développement
des télécommunications (BDT)

Réf.: Circulaire BDT/DNS/CYB/101

Genève, le 10 août 2021

- États Membres de l'UIT
- Membres du Secteur de l'UIT-D
- Établissements universitaires
- Organisations régionales/internationales
- Secteurs nationaux/équipes CERT nationales essentiels
- Coordonnateurs de la cybersécurité de l'UIT

Objet: Invitation à participer à l'édition de 2021 du cyberexercice mondial de l'UIT

Madame, Monsieur,

J'ai l'honneur de vous inviter à participer à l'édition de 2021 du cyberexercice mondial de l'Union internationale des télécommunications (UIT), qui aura lieu de septembre à novembre. À l'image de l'édition de 2020 du cyberexercice mondial, les cyberexercices régionaux de l'UIT seront remplacés par un seul et même cyberexercice virtuel.

Les séances de l'édition de 2021 du cyberexercice mondial, qui mettront plus particulièrement l'accent sur le rôle que jouent les équipes nationales d'intervention en cas d'incident informatique (CIRT) et les équipes nationales d'intervention en cas d'incident de sécurité informatique (CSIRT) dans le renforcement de la cyberrésilience et la protection des infrastructures essentielles de l'information, s'articuleront autour de quatre concepts thématiques: *réflexion, échange, apprentissage* et *mise en pratique*.

Ce cyberexercice virtuel servira de plate-forme de renforcement des capacités pour améliorer les mécanismes de communication existants et renforcer les méthodes de coopération innovantes pour les équipes CIRT/CSIRT nationales. Il comprendra des réunions interrégionales, des webinaires, des formations techniques et des exercices de cybersécurité et offrira un cadre commun permettant de mettre en relation les équipes de cybersécurité des États Membres et des Membres de Secteur de l'UIT, y compris les universités, les organisations régionales ou internationales, les opérateurs de télécommunication, les régulateurs, ainsi que les autres parties prenantes concernées.

Il est recommandé que les organisations participantes soient composées d'une équipe d'au moins deux (2) techniciens et d'un (1) représentant au niveau de la direction. Pour obtenir de plus amples renseignements, veuillez consulter le mandat reproduit ci-joint (Annexe 1) ou consulter la page web de la manifestation, à l'adresse: https://itu.int/go/GCD2021.

Pour toute autre demande de renseignements concernant l'édition de 2021 du cyberexercice mondial de l'UIT, veuillez vous mettre en rapport avec votre coordonnateur régional de l'UIT chargé de la cybersécurité, comme indiqué dans l'Annexe.

J'espère que vous participerez au cyberexercice virtuel.

Veuillez agréer, Madame, Monsieur, l'assurance de ma considération distinguée.

[Original signé]

Doreen Bogdan-Martin
Directrice

ANNEXE 1

Programme de cybersécurité UIT/BDT

Édition de 2021 du cyberexercice mondial de l'UIT

Mandat

Juillet 2021

Mandat

1 INTRODUCTION

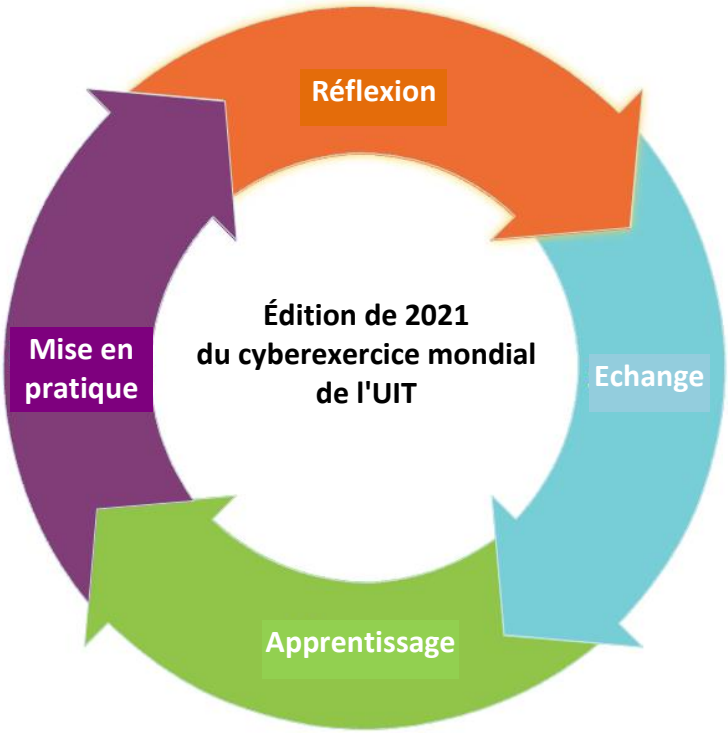
L'Union internationale des télécommunications (UIT) s'efforce d'améliorer les capacités de préparation, de protection et d'intervention en cas d'incident des États Membres en matière de cybersécurité, en organisant des cyberexercices aux niveaux national, régional et mondial. Ces manifestations annuelles consistent à simuler des cyberattaques, des incidents liés à la sécurité de l'information ou d'autres types de dysfonctionnements, en vue de tester les cybercapacités d'une organisation. Au cours des dix dernières années, l'UIT a organisé plus de trente cyberexercices, en partenariat avec plus de 100 pays résolus à améliorer la cybersécurité aux niveaux national et mondial.

Bien que les cyberexercices de l'UIT se déroulent généralement au niveau régional, les éditions de 2020 et 2021 rassemblent des instances s'occupant de cybersécurité, et plus particulièrement les États Membres de l'UIT au niveau mondial, afin de relever les défis consécutifs à la pandémie de COVID-19.

Compte tenu des débats qui ont eu lieu lors de l'édition de 2020 et des résultats de cette manifestation, l'édition de 2021 du cyberexercice mondial sera axée sur le rôle que jouent les équipes nationales d'intervention en cas d'incident informatique (CIRT) et les équipes nationales d'intervention en cas d'incident de sécurité informatique (CSIRT) dans le renforcement de la cyberrésilience et la protection des infrastructures essentielles de l'information.

2 OBJECTIFS

L'édition de 2021 du cyberexercice mondial comprendra des séances qui s'articuleront autour de quatre concepts thématiques: *réflexion, échange, apprentissage* et *mise en pratique*.



- **Réflexion:** Réunir la communauté mondiale de la cybersécurité pour passer en revue les grandes tendances qui se dessinent au niveau régional en matière de cybersécurité et réfléchir aux améliorations possibles compte tenu des cinq piliers du Programme mondial cybersécurité (GCA) et de l'Indice mondial de cybersécurité (GCI) de l'UIT.
- **Échange:** Promouvoir l'échange de connaissances entre les réseaux de bénéficiaires communication ressources et échanger des financement.
- **Apprentissage:** Renforcer les capacités des communautés d'équipes CSIRT en matière d'intervention en cas d'incident et de protection des infrastructures essentielles de l'information (CIIP).
- **Mise en pratique:** Tester les principaux concepts de la résilience opérationnelle auprès des équipes CSIRT/CIRT/CERT.

3 ACTIVITÉS PRÉVUES

Toutes les activités auront lieu en ligne sur une durée de trois mois. Les experts de l'UIT, en coopération avec des partenaires sur le terrain, s'attacheront à organiser et/ou accueillir:

- **Trois (3) réunions interrégionales (*Réflexion*)**: Parmi les intervenants figureront des responsables de la cybersécurité issus de gouvernements, d'organisations régionales, etc., qui échangeront des informations sur les bonnes pratiques et les enseignements tirés en matière de protection des infrastructures essentielles de l'information (CIIP).
  - **Réunion interrégionale I:** régions Asie-Pacifique et CEI
  - **Réunion interrégionale II:** régions Afrique et Europe
  - **Réunion interrégionale III:** régions Amériques et États arabes.
- **Deux (2) webinaires (*Échange*)**:
  - **Webinaire I**: Exploiter le potentiel de la coopération en matière de cybersécurité: Possibilités, défis et perspectives. Les intervenants mettront l'accent sur la grande quantité de ressources disponibles pour les équipes CSIRT, en particulier les mécanismes de financement au sein des organisations internationales.
  - **Webinaire II**: Les femmes dans le secteur de la cybersécurité: un an après, quel bilan?

    En 2021, l'UIT a mis en place le Programme de mentorat "Les femmes dans le secteur de la cybersécurité" (en collaboration avec le Forum FIRST et le partenariat EQUALS). Ce programme fait suite au webinaire consacré à l'autonomisation des femmes en matière de cybersécurité qui a été organisé par l'UIT dans le cadre de l'édition de 2020 du cyberexercice. Il a mis en évidence la nécessité de présenter des personnalités constituant un exemple à suivre et d'élaborer des programmes de mentorat pour augmenter le nombre de dirigeantes dans le domaine de la cybersécurité. Le programme, qui s'appuie sur les initiatives en cours prises par l'UIT pour réduire la fracture numérique entre les hommes et les femmes en intégrant les activités axées sur la parité hommes-femmes, fait appel à des personnalités constituant un exemple à suivre et à des leaders dans ce domaine et les met en relation avec des femmes talentueuses dans le monde entier.

    La première édition du programme a été mise en œuvre avec succès, et la session réunira les mentors, les bénéficiaires du mentorat et les formateurs, pour examiner les incidences du programme, y compris l'échange de témoignages et de bonnes pratiques, dans le cadre d'un effort concerté visant à définir le programme futur et les perspectives qui s'offrent à la communauté pour 2022 et au-delà.
- **Six (6) séances de formation (*Apprentissage*)**: Des experts de l'UIT, en collaboration avec des organisations partenaires, animeront des séances de formation durant la seconde partie du cyberexercice. Les séances de formation se tiendront sur une période de trois semaines. Les thèmes abordés seront les suivants:
  - Comment identifier et classer les actifs et les services des infrastructures essentielles de l'information.
  - Renforcement des cadres juridiques, politiques et de mise en conformité pour les infrastructures essentielles de l'information.
  - Suivi des menaces et intervention en cas d'incident pour les infrastructures nationales essentielles (CNI) au moyen d'outils à code source ouvert.
  - Aspects fondamentaux de l'atténuation des effets des attaques par déni de service réparti (DDOS).
  - Réalisation d'exercices pour renforcer les moyens d'intervention en cas d'incident.
  - Évaluer et améliorer le niveau de maturité des équipes CIRT au niveau national.

- **Six (6) exercices fondés sur des scénarios, (*Mise en pratique*):** Les exercices font partie des temps forts des cyberexercices organisés par l'UIT et sont ouverts aux équipes CIRT/CSIRT nationales/gouvernementales. Les pays participants sont représentés par des équipes composées de deux à quatre personnes et se dérouleront sur deux semaines.

La participation aux trois réunions interrégionales sera réservée aux États Membres des régions concernées. Les autres webinaires, séances de formation et exercices fondés sur des scénarios pourront être suivis par tous les participants, indépendamment de la région à laquelle ils appartiennent.

4 PUBLIC CIBLE

Peuvent participer aux dialogues régionaux, aux webinaires et aux formations les équipes CIRT/CSIRT nationales, les ministères, les régulateurs, les opérateurs de télécommunication, les établissements universitaires et de formation, les constructeurs d'équipements de télécommunication, les instituts de recherche et de conception, les éditeurs de logiciels et d'autres parties intéressées parmi les États Membres et les Membres de Secteur de l'UIT.

5 INSCRIPTION ET LOGISTIQUE

Nous recommandons à tous les participants au cyberexercice d'apporter leur ordinateur ou ordinateur portable, doté d'une connexion Internet stable.

Pour obtenir de plus amples renseignements sur l'édition de 2021 du cyberexercice mondial, veuillez consulter le site web de la manifestation à l'adresse: https://itu.int/go/GCD2021.

Des informations détaillées sur l'inscription, notamment les liens d'accès aux réunions et d'autres renseignements, seront envoyées aux participants via l'adresse électronique qu'ils ont indiquée. L'inscription aux formations et aux exercices prendra fin le 10 septembre 2021, ou lorsque les séances seront complètes.

6 COORDONNÉES

Pour toute question, veuillez contacter votre coordonnateur régional de l'UIT chargé de la cybersécurité:

- Bureau régional pour la région Afrique, M. Serge Valery Zongo (serge.zongo@itu.int)
- Bureau régional pour la région Amériques, M. Pablo Palacios (pablo.Palacios@itu.int)
- Bureau régional pour la région des États arabes, M. Ahmed ElRaghy (ahmed.elraghy@itu.int)
- Bureau régional pour la région Asie-Pacifique, M. Calvin Chan (calvin.chan@itu.int)
- Bureau régional pour la CEI, M. Farid Nakhli (farid.nakhli@itu.int)
- Bureau régional pour la région Europe, M. Jaroslaw Ponder (jaroslaw.ponder@itu.int)

7 CALENDRIER DES ACTIVITÉS

L'ordre du jour sera mis à jour périodiquement sur la page web du cyberexercice. Veuillez consulter le calendrier en ligne pour obtenir des informations détaillées et actualisées: https://itu.int/go/GCD2021.