Bureau de développement
des télécommunications (BDT)

Réf.: Circulaire/BDT/DNS/CYB/051

Genève, le 24 juillet 2020

- 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 2020 du cyberexercice mondial de l'UIT

Madame, Monsieur,

J'ai l'honneur de vous inviter à participer à l'édition de 2020 du cyberexercice mondial de l'Union internationale des télécommunications (UIT), qui aura lieu de septembre à novembre 2020. Le cyberexercice de l'UIT se tiendra de façon virtuelle en raison de la pandémie actuelle de COVID-19 et des risques et restrictions qui en découlent en matière de voyages et de rassemblements.

En raison de la pandémie de COVID-19, le recours aux technologies de l'information et de la communication (TIC) s'est accru partout dans le monde. Les TIC permettent d'être productif et mobilisé tout en respectant les mesures de distanciation sociale. Ce recours accru aux TIC soulève cependant de nombreuses difficultés en matière de cybersécurité et les cybermenaces se multiplient.

Les cyberexercices régionaux de l'UIT qu'il était prévu d'organiser en 2020 seront remplacés par un cyberexercice mondial virtuel. Dans le cadre de ce cyberexercice mondial, nous organiserons pendant trois (3) mois une série de dialogues régionaux, de webinaires internationaux, de séances de formation et d'exercices fondés sur des scénarios, afin de contribuer à renforcer les capacités dont disposent les pays pour mieux gérer les cybermenaces. On trouvera plus de renseignements à ce sujet dans le descriptif de la manifestation joint à la présente lettre (Annexe 1).

Le cyberexercice mondial est une manifestation sur le renforcement des capacités qui vise à améliorer les capacités des équipes participantes en matière de communication et d'intervention en cas d'incident et à encourager 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) à agir ensemble.

Peuvent participer à ce cyberexercice les équipes nationales CIRT/CSIRT, les ministères, les régulateurs, les opérateurs de télécommunication, les universités et les établissements 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 des Secteurs de l'UIT ainsi que les établissements universitaires participant aux travaux de l'Union. Il est recommandé que l'équipe participante soit composée d'au moins deux (2) techniciens et d'un (1) responsable.

Pour obtenir de plus amples renseignements et vous inscrire aux activités du cyberexercice mondial, veuillez cliquer sur le lien suivant: https://www.itu.int/en/ITU-D/Cybersecurity/Pages/Cybedrills-2020.aspx.

Les responsables des priorités thématiques régionales de l'UIT en matière de cybersécurité se tiennent à votre disposition pour toute demande de renseignements concernant les activités de l'édition de 2020 du cyberexercice mondial de l'UIT.

- 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, Mme Rouda Al Amir Ali (Rouda.AlamirAli@itu.int)
- Bureau régional pour la région Asie-Pacifique, M. Sameer Sharma (sameer.sharma@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)

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

[Original signé]

Doreen Bogdan-Martin
Directrice

ANNEXE 1

Édition de 2020 du cyberexercice mondial de l'UIT

1 PRÉSENTATION

L'Union internationale des télécommunications (UIT) améliore les capacités nationales de préparation, de protection et d'intervention en cas d'incident des États en matière de cybersécurité, en organisant des cyberexercices aux niveaux régional et international. Un cyberexercice est une manifestation annuelle consistant 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, qu'il s'agisse de détecter un incident de sécurité ou d'intervenir comme il se doit et d'atténuer autant que possible les conséquences d'un tel dysfonctionnement. Un cyberexercice permet aux participants de valider les politiques, des plans, des procédures, des processus et des capacités de préparation, de prévention, d'intervention, de rétablissement et de continuité des activités. À ce jour, l'UIT a organisé plus de 29 cyberexercices dans le monde entier, afin de renforcer les capacités dans le domaine de la cybersécurité dans le cadre d'une collaboration et d'une coopération régionales.

2 OBJECTIFS

L'édition de 2020 du cyberexercice vise essentiellement à:

- permettre aux acteurs clés des secteurs public et privé qui encadrent leur entreprise, organisation ou secteur de compétence à apprécier la situation pendant un cyberdysfonctionnement;
- rassembler les équipes CERT/CIRT/CSIRT dans le cadre d'un exercice unifié pour renforcer les capacités d'intervention et de rétablissement à l'échelle mondiale;
- tester les principaux concepts de résilience opérationnelle auprès des équipes CSIRT/CIRT/CERT;
- identifier, mettre en pratique et favoriser l'amélioration des processus, procédures, interactions et mécanismes d'échange d'informations existants, ou qu'il faudrait mettre en place, parmi les équipes CERT/CSIRT, les centres d'opérations de sécurité, les organismes, les administrations publiques et les organisations régionales chargées de la gestion des crises ainsi que les organismes de régulation;
- mettre en pratique des mécanismes de coordination et des initiatives d'échange d'informations, et mettre au point des capacités communes d'appréciation de la situation ainsi que des procédures décisionnelles dans les milieux de la cybersécurité en cas de cyberincidents; et,
- attirer l'attention sur d'autres initiatives comprenant des cyberexercices.

3 ACTIVITÉS PRÉVUES

En raison des restrictions en matière de voyages et d'autres mesures importantes prises pour lutter contre la pandémie de COVID-19, les activités du cyberexercice se tiendront en ligne sur une durée de trois (3) mois, de septembre à novembre 2020. Les experts de l'UIT, en coopération avec des partenaires sur le terrain, s'attacheront à organiser et/ou accueillir:

- **Six (6) dialogues régionaux sur les enseignements tirés de la pandémie de COVID-19**:
    a) La pandémie de COVID-19 accroît la pression exercée sur les systèmes nationaux de TIC et les expose parfois davantage aux cyberattaques dirigées contre leurs infrastructures essentielles. Ces dialogues régionaux seront l'occasion pour les représentants des équipes CSIRT/CIRT/CERT de tous les États Membres d'échanger des données d'expérience concernant la gestion des problèmes de cybersécurité pendant la pandémie de COVID-19.

- **Trois (3) webinaires**:

  a) **Autonomisation des femmes en matière de cybersécurité:** ce webinaire réunira des intervenants qui examineront le rôle des femmes dans le domaine de la cybersécurité dans tous les secteurs. Ce webinaire sera ouvert à tous les participants.

  b) **Gestion des cybercrises:** il est essentiel de disposer d'une stratégie spéciale de gestion des cybercrises pour renforcer la cyberrésilience au niveau national. Ce webinaire fera intervenir des experts en matière de gestion des cybercrises. Il sera ouvert à tous les participants.

  c) **Évaluer et améliorer la maturité des équipes CIRT:** ce webinaire portera essentiellement sur l'évaluation et l'amélioration de la maturité, deux axes essentiels qui doivent permettre de promouvoir et de renforcer en permanence les capacités des équipes CIRT. Il fera intervenir des experts possédant une vaste expérience de la collaboration avec les équipes CIRT et sera ouvert à tous les participants.

- **Six (6) séances de formation**:

  a) Des experts de l'UIT, en collaboration avec des organisations partenaires, animeront chacune de ces séances de formation, qui auront lieu des jours différents à une heure définie au préalable. Ces séances de formation seront l'occasion de débattre des moyens propres à renforcer efficacement les capacités de renseignement sur les cybermenaces (CTI), d'intervention en cas d'incident, de communication lors de la gestion des crises, de cybersécurité industrielle et d'intervention en cas d'incident, d'identification des fausses informations et de renseignements sur les cybermenaces dans la pratique. Elles seront ouvertes à tous les participants.

- **Six (6) exercices fondés sur des scénarios**:

  a) Les exercices fondés sur des scénarios font partie des temps forts des cyberexercices de l'UIT. Cette année, l'UIT projette d'organiser six exercices fondés sur des scénarios à des jours différents à une heure déterminée. Ces exercices sont réservés aux équipes CIRT/CSIRT nationales/gouvernementales, et chaque pays participant sera représenté par une équipe composée de deux (2) à quatre (4) participants au plus.

Les webinaires régionaux ayant pour thème "Équipes CIRT et enseignements tirés du COVID-19" ne seront ouverts qu'aux États Membres de la région concernée. 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.

Les exercices sont réservés aux équipes CIRT/CSIRT nationales/gouvernementales et chaque pays inscrit sera représenté par une équipe composée de deux (2) participants.

5 LOGISTIQUE

Nous recommandons à tous les participants d'apporter leur ordinateur ou ordinateur portable, doté d'une connexion Internet stable et adaptée, lorsqu'ils prendront part aux activités du cyberexercice.

6 INSCRIPTION

Pour obtenir davantage d'informations et vous inscrire aux activités, veuillez consulter le site web de la manifestation: https://www.itu.int/en/ITU-D/Cybersecurity/Pages/Cybedrills-2020.aspx.

Des informations détaillées sur les inscriptions, notamment les liens d'accès aux réunions, seront envoyées aux participants via l'adresse électronique qu'ils ont indiquée. L' inscription aux formations et exercices prendra fin le mercredi 30 septembre 2020, ou lorsque les séances seront complètes.

7 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, Mme Rouda Al Amir Ali (Rouda.AlamirAli@itu.int)
- Bureau régional pour la région Asie -Pacifique, M. Sameer Sharma, (sameer.sharma@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)

8 CALENDRIER DES ACTIVITÉS

DIALOGUES RÉGIONAUX

SEPT

- 15 Région Amériques: Équipes CIRT et enseignements tirés de la crise du COVID-19
- 16 Région Asie-Pacifique: Équipes CIRT et enseignements tirés de la crise du COVID-19
- 17 Région Europe: Équipes CIRT et enseignements tirés de la crise du COVID-19
- 22 Région des États arabes : Équipes CIRT et enseignements tirés de la crise du COVID-19
- 23 Région Afrique : Équipes CIRT et enseignements tirés de la crise du COVID-19
- 24 Région de la CEI : Équipes CIRT et enseignements tirés de la crise du COVID-19

WEBINAIRES MONDIAUX

OCT

- 06 Autonomisation des femmes en matière de cybersécurité
- 08 Planification de la gestion des cybercrises: comment réduire les cyberrisques et renforcer la cyberrésilience au niveau national ?

NOV

- 24 Évaluer et améliorer la maturité des équipes CIRT nationales

FORMATIONS AU NIVEAU MONDIAL

OCT

- 13 Comment renforcer efficacement les capacités CTI ?
- 15 Intervention en cas d'incident avec les logiciels TheHive et Cortex
- 20 Communication lors de la gestion des crises
- 22 Cybersécurité industrielle et intervention en cas d'incident

NOV

- 17 Cybermenaces et réseaux sociaux
- 19 Renseignements sur les cybermenaces sur le plan pratique et échange d'informations grâce au logiciel MISP

EXERCICES MONDIAUX

OCT

- 27 Scénario 1
- 28 Scénario 2
- 29 Scénario 3

NOV

- 03 Scénario 4
- 04 Scénario 5
- 05 Scénario 6

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://www.itu.int/en/ITU-D/Cybersecurity/Pages/Cybedrills-2020.aspx.