Documents d'information sur l'UIT

UIT: INSTAURER LA CONFIANCE DANS LES TIC ET LE CYBERESPACE

Le GCA appuie les efforts déployés par l'UIT en vue de créer les capacités techniques nécessaires pour permettre aux pays de lutter contre les cybermenaces, recommande des normes mondiales sur la cybersécurité et les technologies, et sert de plate-forme d'échange de connaissances et d'examen des politiques publiques.

Selon les prévisions de l'UIT, le monde comptera près de trois milliards d'internautes à la fin de 2014, ce qui ouvre de nouvelles perspectives réjouissantes en ce qui concerne l'accès à l'information et les communications. Cependant, les problèmes de sécurité et les failles des réseaux et des services exposent les utilisateurs, partout dans le monde, à des cybermenaces de plus en plus élaborées. L'usurpation d'identité, le spam, les logiciels malveillants, l'exploitation des enfants et d'autres catégories vulnérables et les préjudices qui leur sont causés, peuvent tous avoir des conséquences dramatiques et parfois dévastatrices dans le monde réel, outre les 400 milliards de dollars de perte qu'ils coûteraient chaque année à l'économie mondiale[1].

Les technologies de l'information et de la communication (TIC) étant désormais une infrastructure nationale essentielle, leur perturbation peut s'avérer catastrophique en entraînant l'interruption de services fondamentaux. De plus, au sein d'un environnement large bande connecté en permanence, accessible n'importe quand et n'importe où, des attaques peuvent avoir lieu dans un pays – ou même dans plusieurs pays en même temps – alors que leur auteur se trouve dans une tout autre partie du monde.

Les cybermenaces sont devenues un risque pour tous les pays, même les plus évolués sur le plan technique. Une meilleure coopération internationale peut contribuer à atténuer ce risque.

UNE MENACE INTERNATIONALE GRANDISSANTE

- Près de 400 millions de personnes ont été victimes de cybermenaces en 2013.
- Les campagnes d'attaque ciblées ont augmenté de 91% en 2013, tandis que le nombre d'infractions a augmenté de 62%, et que 38% des utilisateurs mobiles ont été confrontés à la cybercriminalité.
- Le nombre «d'identités exposées» a plus que quintuplé en l'espace d'un an, passant de 93 millions en 2012 à 552 millions en 2013.
- Les trois secteurs les plus exposés aux attaques ciblées sont les pouvoirs publics, l'industrie minière et l'industrie manufacturière (Source: Symantec, 2014 Internet Security Threat Report).

Les utilisateurs mobiles stockent souvent des fichiers sensibles en ligne (52%), stockent des informations professionnelles et personnelles sur les mêmes comptes de stockage en ligne (24%), communiquent fréquemment leurs identifiants et leurs mots de passe à des parents (21%) ou à des amis (18%), autant de pratiques qui mettent en danger leurs données et celles de leur employeur. D'après Symantec, partenaire de l'UIT, seuls 50% des utilisateurs prennent ne serait-ce que des précautions de base en matière de sécurité.

1. McAfee

L'Initiative de l'UIT pour la protection en ligne des enfants (COP) est un réseau international de collaboration qui vise, au moyen de mesures appropriées, à identifier les risques et les vulnérabilités auxquels sont exposés les enfants du monde entier dans le cyberespace, à mieux faire connaître la question de la protection en ligne des enfants, à faciliter la mise en commun des ressources, ainsi qu'à élaborer des outils pratiques destinés à réduire au maximum les risques et à promouvoir une citoyenneté numérique responsable.

Alors que l'«Internet des objets» se concrétise, avec l'interconnexion de millions de dispositifs et l'échange d'informations de machine à machine sans qu'aucune intervention humaine ne soit nécessaire, il devient de plus en plus difficile de distinguer la frontière entre monde physique et monde virtuel. L'UIT, qui rassemble des parties prenantes diverses au sein de partenariats mondiaux, joue un rôle de pointe dans la recherche de solutions techniques et politiques pour lutter contre les problèmes de cybersécurité.

Une étape décisive a été la création, sous les auspices de l'UIT, d'un cadre mondial de coopération appelé Programme mondial cybersécurité (GCA). Le GCA appuie les efforts déployés par l'UIT en vue de créer les capacités techniques nécessaires pour permettre aux pays de lutter contre les cybermenaces, recommande des normes mondiales sur la cybersécurité et les technologies, et sert de plate-forme d'échange de connaissances et d'examen des politiques publiques.

Lutte contre les cyberattaques nationales

Une cyberattaque nationale peut venir gravement perturber les infrastructures essentielles, et avoir des répercussions directes sur le quotidien de la population: impossibilité d'accès aux comptes bancaires, perturbation des réseaux de transport, pannes d'électricité, communications bloquées, et pire encore.

Il est clairement nécessaire d'établir des structures institutionnelles efficaces pour faire face aux cyberincidents et aux cyberattaques. L'UIT collabore avec les Etats Membres et les régions, ainsi qu'avec des partenaires industriels, en vue de déployer des moyens de renforcer les capacités aux niveaux national et régional.

L'UIT œuvre au renforcement des capacités et des compétences dans le cadre de vastes programmes de formation et de soutien. Citons à ce titre les initiatives suivantes:

- Cinquante pays ont bénéficié d'une aide pour évaluer leur état de préparation dans le domaine de la cybersécurité et leur capacité de réaction au niveau national. Sept Etats Membres ont reçu l'aide de l'UIT pour créer une équipe nationale d'intervention en cas d'incident informatique (CIRT), et sept autres sont actuellement engagés dans ce processus.

- A ce jour, sept cyberexercices sur les équipes CIRT ont été organisés, avec la participation de plus de 60 pays. Ces exercices ont pour but de vérifier si les fonctions fondamentales des équipes CIRT en place sont conformes aux normes et aux bonnes pratiques internationales.

- La mise en place de stratégies nationales de cybersécurité est particulièrement difficile pour les pays les moins avancés (PMA), qui ne disposent pas de cadres juridiques et réglementaires appropriés, et dont les capacités humaines/compétences et les ressources financières pour identifier et contrer les cybermenaces sont limitées. Le projet de l'UIT intitulé Renforcer la cybersécurité dans les pays les moins avancés vise à aider les PMA à renforcer leurs capacités en matière de cybersécurité, afin de garantir une meilleure protection de leur infrastructure nationale et d'optimiser les avantages socioéconomiques qui en résultent.

La sécurité occupe une place fondamentale dans les Recommandations et les normes de l'UIT, et toutes les commissions d'études de l'UIT ont maintenant l'habitude d'examiner les questions relatives à la sécurité dans le cadre de leurs travaux.

- Les centres régionaux de cybersécurité de l'UIT offrent une assistance supplémentaire au niveau régional. Il s'agit de centres physiques hébergés par un Etat Membre qui joue alors le rôle de coordonnateur régional de l'UIT pour les questions de cybersécurité. Le Centre régional de cybersécurité pour la région des Etats arabes se situe à Oman, tandis qu'un projet de création d'un centre régional de cybersécurité pour l'Afrique au Nigéria est en cours.

- L'UIT aide les Etats Membres à comprendre les aspects juridiques de la cybersécurité, afin de contribuer à l'harmonisation de leurs cadres juridiques, en rendant ces cadres applicables et interopérables au niveau international.

- Compte tenu du rôle grandissant joué par les TIC dans des services aussi variés que la santé, l'éducation, la finance et le commerce, il devient de plus en plus urgent de se doter d'un cyberenvironnement entièrement sécurisé. Pourtant, le monde souffre d'une pénurie chronique de professionnels de la cybersécurité qualifiés. Pour contribuer à combler ce vide, l'UIT a organisé des ateliers de formation à la cybersécurité pour plus de 1 900 fonctionnaires, régulateurs et professionnels des TIC issus des secteurs public et privé dans le monde.

Protection en ligne des enfants (COP)

Les enfants constituent l'un des groupes les plus vulnérables en ligne. La nouvelle génération d'utilisateurs nés avec le numérique, lesquels sont beaucoup plus enclins à divulguer leurs données personnelles en ligne, offre une cible facile aux cybercriminels et aux pirates.

La frontière entre le monde physique et le monde en ligne est de plus en plus perméable, ce qui a de graves incidences sur le bien-être physique et mental des enfants. Dans une enquête récente, près de la moitié des adolescents âgés de 13 à 17 ans ont dit avoir été victimes d'intimidations en ligne au cours de l'année écoulée. Plus inquiétant encore, trois quarts des jeunes ayant fait l'objet de sollicitations sexuelles agressives dans le monde réel avaient rencontré leur agresseur en ligne.

L'Initiative de l'UIT pour la protection en ligne des enfants (COP) est un réseau international de collaboration qui vise, au moyen de mesures appropriées, à identifier les risques et les vulnérabilités auxquels sont exposés les enfants du monde entier dans le cyberespace, à mieux faire connaître la question de la protection en ligne des enfants, à faciliter la mise en commun des ressources, ainsi qu'à élaborer des outils pratiques destinés à réduire au maximum les risques et à promouvoir une citoyenneté numérique responsable. Dans le cadre de l'initiative COP, plus de 54 partenaires internationaux issus des pouvoirs publics, du secteur privé, de la société civile, des établissements universitaires et des organisations internationales, collaborent pour atteindre ces buts.

Normes techniques (Recommandations)

Les normes techniques de l'UIT (connues sous le nom de recommandations) jouent un rôle essentiel dans la protection en ligne des utilisateurs. La Commission d'études 17 de l'UIT-T est la commission d'études directrice pour la sécurité des télécommunications et la gestion d'identité, avec pour objectif principal le renforcement de la confiance et de la sécurité dans l'utilisation des TIC.

La sécurité occupe une place fondamentale dans les Recommandations et les normes de l'UIT, et toutes les commissions d'études de l'UIT ont maintenant l'habitude d'examiner les questions relatives à la sécurité dans le cadre de leurs travaux. Les résultats obtenus à ce jour incluent des Recommandations techniques pour les réseaux utilisant le protocole Internet (IP), des normes relatives aux réseaux de prochaine génération (NGN), et la mise en place de principes de sécurité clairs pour les réseaux cellulaires mobiles existants et futurs. Un exemple remarquable est la Recommandation UIT-T **X.509**, qui à trait aux infrastructures de clé publique (PKI) et aux infrastructures de gestion des privilèges (PMI). Cette Recommandation spécifie, entre autres, des formats normalisés pour les certificats de clé publique, les listes de révocation de certificat et les certificats d'attribut.

Une approche mondiale multi-parties prenantes

- Du fait de la dépendance croissante vis-à-vis des TIC dans les pays les moins avancés (PMA), la cybersécurité devient une priorité de plus en plus urgente. En effet, d'après les études, les pays en développement sont les plus vulnérables à la cybercriminalité et aux cybermenaces. Le projet de l'UIT intitulé Renforcer la cybersécurité dans les pays les moins avancés vise à protéger les utilisateurs et à rendre l'Internet plus sûr en fournissant une assistance au niveau des politiques.

- L'UIT a conclu un partenariat avec ABI Research concernant l'Indice de la cybersécurité dans le monde (GCI), afin de fournir des points de repère sur les capacités nationales en matière de cybersécurité et de permettre aux Etats Membres de profiter des bonnes pratiques.

- En outre, l'UIT a mis en place une coopération officielle avec des entreprises s'occupant de cybersécurité, comme Symantec et Trend Micro, pour partager sur le long terme des informations concernant l'évolution actuelle et future des cybermenaces dans le monde.

- L'UIT collabore avec d'autres institutions/organes de la famille des Nations Unies, en vue d'améliorer la coordination au sein du système des Nations Unies concernant l'aide aux Etats Membres dans le domaine de la cybersécurité.