|  |  |
| --- | --- |
| **Bureau de la normalisationdes télécommunications** | **logo_F_** |
|  |  |

 Genève, le 30 septembre 2013

|  |  |  |
| --- | --- | --- |
| Réf.:Tél.:Télécopie:Courriel: | **Circulaire TSB 52**COM 17/MEU+41 22 730 5866+41 22 730 5853tsbsg17@itu.int | - Aux administrations des Etats Membres de l'Union |
|  |  | **Copie**:- Aux Membres du Secteur UIT-T;- Aux Associés de l'UIT-T;- Aux établissements universitaires participant aux travaux de l'UIT-T;- Aux Président et Vice-Présidents de la Commission d'études 17;- Au Directeur du Bureau de développement des télécommunications;- Au Directeur du Bureau desradiocommunications |

|  |  |
| --- | --- |
| Objet: | **Réunion de la Commission d'études 17 en vue d'approuver les projets de nouvelle Recommandation UIT-T X.1210, X.1243 Cor.1, X.1546, X.1582 et X.1600 et les projets de Recommandation révisée UIT-T X.1520 et X.1526, conformément aux dispositions de la Section 9 de la Résolution 1 de l'AMNT (Dubaï, 2012)****Genève, le 24 janvier 2014** |

Madame, Monsieur,

1 A la demande du Président de la Commission d'études 17, *Sécurité*, j'ai l'honneur de vous informer que ladite Commission d'études, qui se réunira du 15 au 24 janvier 2014, a l'intention d'appliquer la procédure décrite dans laSection 9 de la Résolution 1 de l'AMNT (Dubaï, 2012) pour l'approbation des projets de Recommandation et du projet de corrigendum mentionnés ci-dessus.

2 Vous trouverez dans l'**Annexe 1** le titre, le résumé et la localisation des projets de Recommandation UIT-T proposés pour approbation.

3 Tout Etat Membre, Membre de Secteur, Associé de l'UIT ou établissement universitaire participant aux travaux de l'UIT constatant qu'un brevet, dont lui ou une autre organisation est titulaire, couvre peut-être, en totalité ou en partie, des éléments des projets de Recommandation qu'il est proposé d'approuver est invité à communiquer ces renseignements au TSB, conformément à la politique commune de l'UIT-T, l'UIT-R, l'ISO et la CEI en matière de brevets.

Les renseignements existants sur les brevets sont accessibles en ligne sur le site web de l'UIT‑T ([www.itu.int/ITU-T/ipr/](http://www.itu.int/ITU-T/ipr/)).

4 Compte tenu des dispositions de laSection 9 de la Résolution 1, je vous serais reconnaissant de bien vouloir me faire savoir au plus tard **le 3 janvier 2014**à 24 heures UTC si votre Administration autorise la Commission d'études 17 à examiner, lors de sa réunion, lesdits projets de Recommandation et de corrigendum aux fins d'approbation.

Si des Etats Membres estiment que la procédure d'approbation ne doit pas se poursuivre, ils sont invités à faire connaître leurs raisons et à proposer les modifications susceptibles de permettre la reprise des procédures d'examen et d'approbation des projets de Recommandation et de corrigendum.

5 Si au moins 70% des réponses des Etats Membres sont en faveur de l'examen, aux fins d'approbation, de ces projets de Recommandation et de corrigendum lors de la réunion de la Commission d'études, une séance plénière se tiendra **le 24 janvier 2014** pour appliquer la procédure d'approbation.

En conséquence, j'invite votre Administration à se faire représenter à cette réunion. Les **Administrations des Etats Membres de l'Union** sont invitées à communiquer le nom du Chef de leur délégation. Si votre Administration souhaite se faire représenter à cette réunion par une exploitation reconnue, un organisme scientifique ou industriel, ou une autre entité s'occupant de questions de télécommunications, le Directeur doit en être informé, conformément à l'article 19, numéro 239, de la Convention de l'UIT.

6 L'ordre du jour ainsi que tous les renseignements pertinents concernant la réunion de la Commission d'études 17 seront disponibles dans la Lettre collective 3/17.

7 Après la réunion, le Directeur du TSB fera connaître, par voie de circulaire, la décision prise au sujet de ces Recommandations. Cette information sera également publiée dans le Bulletin d'exploitation de l'UIT.

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

Malcolm Johnson
Directeur du Bureau de la
normalisation des télécommunications

**Annexe**: 1

**ANNEXE 1
(de la Circulaire TSB 52)**

**Résumé et localisation des textes**

Projet de nouvelle Recommandation UIT-T X.1210 (X.trm), Description générale de mécanismes de résolution des problèmes de sécurité à la source dans les réseaux fondés sur le protocole Internet
COM 17 – R 12

Résumé

Les mécanismes de résolution des problèmes de sécurité à la source dans les réseaux fondés sur le protocole Internet font intervenir des techniques visant à découvrir des informations techniques concernant les points d'entrée, les trajets complets ou partiels ou la source d'un ou de paquets à l'origine d'un problème dans un réseau, généralement aux fins de la résolution de ce problème.

La Recommandation UIT-T X.1210 présente une description de mécanismes de résolution des problèmes de sécurité à la source, ainsi que des critères de sélection et des lignes directrices de base concernant ces mécanismes.

Projet de nouveau Corrigendum 1 à la Recommandation UIT-T X.1243, Système de passerelle interactive pour lutter contre le spam: Corrigendum 1
COM 17 – R 13

Résumé

Le Corrigendum 1 à la Recommandation UIT-T X.1243 (2010) contient les corrections de deux erreurs dans le § 7.2.7.

Projet de Recommandation révisée UIT-T X.1520 (X.cve), Vulnérabilités et expositions courantes
COM 17 – R 14

Résumé

La Recommandation UIT-T X.1520 relative à l'utilisation des vulnérabilités et expositions courantes (CVE, *common vulnerabilities and exposures*) traite d'un moyen structuré d'échange d'informations sur les vulnérabilités et les expositions en matière de sécurité de l'information, qui fournit des dénominations communes pour les problèmes connus du public rencontrés dans les logiciels commerciaux ou libres utilisés dans les réseaux de communication, dans les dispositifs d'utilisateur final, ou dans tout autre type de dispositif des technologies de l'information et de la communication (TIC) utilisant des logiciels. Cette Recommandation vise à définir l'utilisation des CVE pour faciliter l'échange de données sur les vulnérabilités entre différentes capacités (outils, répertoires et services) sur la base de ces dénominations communes. Elle définit l'utilisation des CVE en vue d'offrir un mécanisme pour permettre d'utiliser en association des bases de données sur les vulnérabilités et d'autres capacités, d'une part, et de faciliter la comparaison des outils et services de sécurité, d'autre part. Cette Recommandation ne prend pas en considération les informations telles que des informations sur les risques, les incidences et les solutions, ou des informations techniques détaillées. Elle prend uniquement en considération le numéro d'identification standard avec un indicateur d'état, une brève description, et des références aux rapports et avis de vulnérabilité associés. Le répertoire des identifiants de CVE est disponible à l'adresse: [[cve.mitre.org/cve/cve.html](file:///%5C%5Cblue%5Cdfs%5Cpool%5CFRA%5CITU-T%5CBUREAU%5CCIRC%5C000%5Ccve.mitre.org%5Ccve%5Ccve.html)].

Le but des CVE, dont l'utilisation est définie dans cette Recommandation, est de pouvoir identifier toutes les vulnérabilités et expositions connues du public. Cette Recommandation est conçue pour prendre en considération des informations bien établies, mais l'objectif premier est d'identifier les vulnérabilités et les expositions qui sont détectées par les outils de sécurité ainsi que tout nouveau problème rendu public, puis de régler les éventuels problèmes de sécurité plus anciens qui nécessitent une validation.

Projet de Recommandation révisée UIT-T X.1526 (X.oval), Langage ouvert d'évaluation de la vulnérabilité
COM 17 – R 15

Résumé

La Recommandation UIT-T X.1526 sur le langage ouvert d'évaluation de la vulnérabilité (OVAL, *open vulnerability and assessment language*) normalise les trois principales étapes du processus d'évaluation: la représentation des informations de configuration des points d'extrémité à tester; l'analyse du point d'extrémité en vue de détecter un état précis de la machine (en ce qui concerne la vulnérabilité, la configuration, un correctif, etc.); et le compte-rendu des résultats de cette évaluation. OVAL a pour objet de fournir une norme communautaire internationale en matière de sécurité de l'information, qui vise à promouvoir des contenus ouverts et publiquement accessibles sur la sécurité et à normaliser le transfert de ces informations à l'ensemble des outils et des services de sécurité. Par OVAL, on entend le langage employé pour coder des informations précises sur le point d'extrémité, mais aussi un ensemble de divers répertoires de contenus, tenus dans l'ensemble de la communauté.

**Projet de nouvelle Recommandation UIT-T X.1546 (X.maec), Liste et caractérisation des attributs de logiciels malveillants
COM 17 – R 16**

Résumé

Le langage de liste et de caractérisation des attributs de logiciels malveillants (MAEC) comprend des listes d'attributs et de comportements de logiciels malveillants qui fournissent un vocabulaire commun. Ces listes sont à des niveaux différents d'abstraction: données observables de bas niveau, comportements de niveau intermédiaire et taxonomies de haut niveau. La Recommandation UIT-T X.1546, qui définit la version initiale du MAEC, porte essentiellement sur la création de la liste d'attributs de bas niveau des logiciels malveillants, et exploite les quelques travaux analogues qui ont déjà été effectués dans ce domaine. Cette Recommandation permettra ainsi, dans un premier temps, de caractériser les types de logiciels malveillants les plus courants, y compris les chevaux de Troie, les vers informatiques et les outils de dissimulation d'activité, et pourra ensuite être appliquée à des types de logiciels malveillants plus spécifiques.

**Projet de nouvelle Recommandation UIT-T X.1582 (X.cybex-tp), Protocoles de transport prenant en charge l'échange d'informations sur la cybersécurité**

**COM 17 – R 17**

Résumé

Cette Recommandation donne une vue d'ensemble des protocoles de transport qui ont été adoptés et adaptés pour être utilisés dans le cadre de l'échange d'informations sur la cybersécurité (CYBEX). Elle présente des applications de transport ainsi que des caractéristiques des protocoles de transport et contient des considérations relatives à la sécurité.

**Projet de nouvelle Recommandation UIT-T X.1600 (X.ccsec), Cadre de sécurité applicable à l'informatique en nuage
COM 17 – R 19**

Résumé

La recommandation UIT-T X.1600 décrit le cadre de sécurité applicable à l'informatique en nuage. Elle présente une analyse des menaces et des problèmes de sécurité dans l'environnement de l'informatique en nuage et décrit les capacités de sécurité qui pourraient atténuer ces menaces et résoudre les problèmes de sécurité. Elle présente une méthode générale permettant de déterminer, parmi ces capacités de sécurité, celles qu'il faudra spécifier pour atténuer les menaces et résoudre les problèmes de sécurité dans le cadre de l'informatique en nuage. L'Appendice I contient un tableau mettant en correspondance, pour une menace ou un problème donné, la ou les capacités de sécurité à mettre en oeuvre.

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