|  |  |
| --- | --- |
| **Bureau de la normalisation des télécommunications** | **logo_F_** |
|  |  |

Genève, le 7 janvier 2011

|  |  |  |
| --- | --- | --- |
| Réf.:  Tél.: Fax: E-mail: | **Circulaire TSB 158**  COM 17/MEU  +41 22 730 5866 +41 22 730 5853 [tsbsg17@itu.int](mailto:tsbsg17@itu.int) | - Aux administrations des Etats Membres de l'Union |
|  |  | **Copie**:  - Aux Membres du Secteur UIT-T;  - Aux Associés 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 des radiocommunications |

|  |  |
| --- | --- |
| Objet: | **Réunion de la Commission d'études 17 en vue d'approuver les projets de nouvelle Recommandation UIT-T X.1261, X.1500, X.1520 et X.1521, conformément aux dispositions de la Section 9 de la Résolution 1 de l'AMNT (Johannesburg, 2008)**  **Genève, le20 avril 2011** |

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 11 au 20 avril 2011, a l'intention d'appliquer la procédure décrite dans laSection 9 de la Résolution 1 de l'AMNT (Johannesburg, 2008) pour l'approbation des projets de nouvelle Recommandation mentionnés ci‑dessus.

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

3 Tout Etat Membre, Membre de Secteur ou Associé 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 30 mars 2011** à 24 heures UTC si votre Administration autorise la Commission d'études 17 à examiner, lors de sa réunion, lesdits projets de nouvelle Recommandation 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 nouvelle Recommandation.

5 Si au moins 70% des réponses des Etats Membres sont en faveur de l'examen, aux fins d'approbation, de ces projets de nouvelle Recommandation lors de la réunion de la Commission d'études, une séance plénière se tiendra **le 20 avril 2011** 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 5/17.

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 158)

**Résumé et localisation des textes**

Projet de nouvelle Recommandation UIT-T X.1500 (X.cybex), Techniques d'échange d'informations sur la cybersécurité   
COM 17 – R 25 *(bientôt disponible sur le web)*

Résumé

Cette Recommandation décrit des techniques d'échange d'informations sur la cybersécurité. Utilisables séparément ou de manière combinée, selon les souhaits ou les besoins, ces techniques visent à améliorer la cybersécurité grâce à un échange d'informations cohérent, complet, global, garanti et en temps utile. Cette Recommandation n'entraîne aucune obligation quant à l'échange d'informations, et elle ne traite ni des moyens d'acquisition ni de l'utilisation finale des informations.

Projet de nouvelle Recommandation UIT-T X.1520 (X.cve), Vulnérabilités et expositions courantes (CVE)  
COM 17 – R 26

Résumé

Cette Recommandation traite d'un moyen structuré d'échange d'informations sur les vulnérabilités et les expositions courantes (CVE, *common vulnerabilities and exposures*) en matière de sécurité de l'information, le but étant de fournir 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 faciliter l'échange de données sur les vulnérabilités entre différentes capacités (outils, répertoires et services) sur la base de ces dénominations communes. Elle est conçue pour permettre d'interconnecter des bases de données sur les vulnérabilités et autres capacités, et pour faciliter la comparaison des outils et services de sécurité. En tant que telle, 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 but de 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 nouvelle Recommandation UIT-T X.1521 (X.cvss), Système d'évaluation des vulnérabilités courantes (CVSS)  
COM 17 – R 27 *(bientôt disponible sur le web)*

Résumé

Cette Recommandation établit un cadre ouvert pour la communication des caractéristiques et des incidences des vulnérabilités en matière de technologies de l'information et de la communication (TIC) rencontrées 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 TIC utilisant des logiciels. Elle présente un système d'évaluation des vulnérabilités courantes (CVSS, *common vulnerabilty scoring system*), dont le but est de permettre aux gestionnaires des TIC, aux fournisseurs de bulletins d'information sur les vulnérabilités, aux fournisseurs de systèmes de sécurité, aux fournisseurs d'application et aux chercheurs d'utiliser un langage commun en ce qui concerne l'évaluation des vulnérabilités en matière de TIC.

**Projet de nouvelle Recommandation UIT-T X.1261 (X.EVcert), Cadre applicable aux certificats de validation étendue (EVcert)  
COM 17 – R 30**

Résumé

Cette Recommandation établit un cadre applicable aux certificats de validation étendue. Elle décrit les exigences minimales en matière de technologies, protocoles, vérification d'identité, gestion du cycle de vie et méthodes d'audit qui doivent être satisfaites pour pouvoir délivrer et gérer des certificats de validation étendue ("certificats EV") concernant une organisation. Des informations sur l'organisation concernée découlant de "certificats EV" valables peuvent alors être présentées de manière spéciale par certains logiciels (par exemple un navigateur) afin de fournir aux utilisateurs une confirmation fiable de l'identité de l'entité qui contrôle le site web ou d'autres services auxquels ils accèdent. Ces extensions sont initialement destinées à être utilisées pour l'établissement de conduits de communication de données sur le web via les protocoles TLS/SSL (*transport layer security/secure socket layer*), mais il est envisagé de les utiliser également pour les extensions S/MIME (*secure/multipurpose Internet mail extensions*), l'horodatage, la téléphonie IP (VoIP, *voice over Internet protocol*), la messagerie instantanée (IM, *instant messaging*), les services web, etc.

Dans cette Recommandation, les principaux objectifs sont: 1) d'identifier l'entité juridique qui contrôle un site web ou de service, et 2) de permettre des communications chiffrées avec ce site. Les objectifs secondaires sont notamment d'améliorer nettement la cybersécurité en facilitant la détermination de la légitimité d'une organisation qui déclare exploiter un site web, et d'établir un cadre qui peut être utilisé pour faciliter la résolution de problèmes liés à la distribution de logiciels malveillants, à l'hameçonnage, au vol d'identité, et à diverses formes de fraude en ligne.

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