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

Genève, le 9 septembre 2011

|  |  |  |
| --- | --- | --- |
| Réf.:  Tél.: Fax: E-mail: | **Circulaire TSB 228**  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 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 des radiocommunications |

|  |  |
| --- | --- |
| Objet: | **Réunion de la Commission d'études 17 en vue d'approuver les projets de nouvelle Recommandation UIT-T X.1037, X.1500.1, X.1524 et X.1541, conformément aux dispositions de la Section 9 de la Résolution 1 de l'AMNT (Johannesburg, 2008)**  **Genève, le 2 mars 2012** |

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 20 février au 2 mars 2012, 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, 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 8 février 2012** 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 2 mars 2012** 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 7/17.

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 228)

Résumé et localisation des textes

Projet de nouvelle Recommandation UIT-T X.1037 (X.rev), Systèmes architecturaux pour les contrôles de sécurité destinés à empêcher les activités frauduleuses dans les réseaux publics des transporteurs  
COM 17 – R 41

Résumé

La Recommandation UIT-T X.1037 décrit une méthodologie pour les systèmes d'évaluation des contrôles de sécurité destinés à empêcher les activités frauduleuses, et donne des critères de sélection de ces systèmes, pour ce qui est des caractéristiques architecturales des réseaux des fournisseurs de services de communication (CSP, *communications service provider*) tels qu'ils sont à ce jour. La Recommandation comporte des méthodes techniques permettant d'aborder la question des contrôles de sécurité et d'évaluer les pertes causées par les activités frauduleuses et contient aussi des lignes directrices quant à l'échange d'informations liées aux activités frauduleuses.

Projet de Recommandation UIT-T X.1500.1 (X.cybex.1), Procédures d'enregistrement d'arcs avec l'arc d'identificateur d'objet aux fins de l'échange d'informations de cybersécurité  
COM 17 – R 42

Résumé

Cette Recommandation porte sur l'enregistrement d'arcs d'identificateur d'objet (OID, *objet identifier*) qui permettent une identification cohérente, unique et mondiale des informations de cybersécurité ainsi que des organismes s'échangeant ces informations et des politiques associées. Cette Recommandation spécifie les informations et les justifications devant être fournies lors de la demande d'une identification OID aux fins de l'échange d'informations de cybersécurité et les procédures appliquées par l'organisme d'enregistrement.

Projet de Recommandation UIT-T X.1524 (X.cwe), Liste des failles courantes  
COM 17 – R 43

Résumé

Cette Recommandation sur l'emploi de la liste des failles courantes (CWE, *common weakness enumeration*) contient une méthode structurée, permettant de s'échanger les failles en matière de sécurité des informations, qui fournit les noms courants des problèmes connus du public, présents dans les logiciels commerciaux ou libres, utilisés dans les réseaux de communication, dans les dispositifs d'utilisateur final ou dans tout autre équipement employant la technologie de l'information et de la communication (TIC), qui assure l'exploitation d'un logiciel. La liste CWE a pour objet de rendre possible une discussion, une description, un choix et un emploi plus efficaces d'outils et de services de sécurité logicielle, qui permettent de repérer les failles dans le code source et dans les systèmes opérationnels, ainsi qu'une compréhension et une gestion meilleures des failles logicielles liées à l'architecture et à la conception. Cette Recommandation indique comment employer la liste CWE pour mettre au point un système permettant d'employer simultanément les outils et les services de sécurité logicielle, les connaissances de base en la matière et d'autres capacités, et pour faciliter la comparaison desdits outils et services de sécurité. La liste CWE offre aussi des informations complémentaires sur les risques éventuels, les impacts, la résolution, et des informations techniques détaillées sur les conséquences possibles des failles logicielles pour un système logiciel. Le répertoire des identificateurs CWE et les informations corollaires associées sont disponibles à l'adresse [cwe.mitre.org/data] en format XML ou pdf. Une version du même contenu, accessible par Internet, est disponible à l'adresse [http://cwe.mitre.org/data/slices/2000.html].

L'objectif de la liste CWE, dont l'emploi est décrit dans cette Recommandation, est d'être exhaustive en pour ce qui est de l'architecture logicielle, la conception, le codage et les erreurs de déploiement qui sont la cause profonde des vulnérabilités et des expositions. Tandis que la liste CWE est conçue pour contenir des informations solides, elle a pour principal objet de recenser, de faire connaître et de décrire cette cause profonde des vulnérabilités et des expositions, de manière que celles-ci puissent être évitées par les développeurs, éprouvées pour les équipes de développement et gérées par elles, et être systématiquement signalées par les outils et les services de sécurité.

**Projet de Recommandation UIT-T X.1541 (X.iodef), Format d'échange de description d'objet incident  
COM 17 – R 44**

Résumé

Le format d'échange de description d'objet incident (IODEF, *incident object description exchange format*) est une représentation des données qui offre un cadre au partage des informations sur les incidents en matière de sécurité informatique que s'échangent couramment les équipes d'intervention en cas d'incident relatif à la sécurité informatique (CSDIRT, *computer security incident response team*). Cette Recommandation décrit le modèle d'information pour le format IODEF et fournit un modèle de données associé, spécifié pour le format XML.

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