|  |  |  |
| --- | --- | --- |
| itu_logo | **Union internationale des télécommunications****Bureau de la Normalisation des Télécommunications** |  |
|  |  |

 Genève, le 21 octobre 2015

|  |  |  |
| --- | --- | --- |
| Réf.:Tél.:Fax:E-mail: | **Circulaire TSB 174**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;- 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.1247, X.1256, X.1257, X.1602 et X.1642, ainsi que le projet de Recommandation révisée UIT-T X.1521, conformément aux dispositions de la Section 9 de la Résolution 1 de l'AMNT (Dubaï, 2012), Genève, 23 mars 2016** |

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 14 au 23 mars 2016, a l'intention d'appliquer la procédure décrite dans la Section 9 de la Résolution 1 de l'AMNT (Dubaï, 2012) pour l'approbation du projet de Recommandation révisée et des projets de nouvelle Recommandation mentionnés ci-dessus.

2 Vous trouverez dans l'**Annexe 1** le titre, le résumé et la localisation du projet de Recommandation UIT-T révisée et 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 2 mars 2016** à 24 heures UTC si votre Administration autorise la Commission d'études 17 à examiner, lors de sa réunion, lesdits projets de Recommandation révisée et nouvelle 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 du projet d'amendement.

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 nouvelle et révisée lors de la réunion de la Commission d'études, une séance plénière se tiendra **le 23 mars 2016** 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.

Chaesub Lee
Directeur du Bureau de la
normalisation des télécommunications

**Annexe**:1

ANNEXE 1
(de la Circulaire TSB 174)

Résumé et localisation des textes

Projet de nouvelle Recommandation UIT-T X.1247 (X.tfcmm), Cadre technique de lutte contre le spam par messagerie mobile
COM 17 – R 50

Résumé

Le spam par messagerie mobile prolifère de manière spectaculaire à mesure que se développent rapidement les services de messagerie mobile. Malheureusement, aucune mesure, à ce jour, ne s'est avérée être une panacée contre ce problème; il est donc nécessaire de mettre en place un cadre pratique de lutte contre le spam. La Recommandation UIT-T X.1247 offre un aperçu des procédés anti-spam existants et propose un cadre technique de lutte contre le spam par messagerie mobile. Ce cadre spécifie les fonctions des entités et les procédures de traitement à adopter. En outre, cette Recommandation propose des mécanismes de partage des informations pour lutter contre les spams par messagerie mobile au sein du domaine de traitement anti-spam ou entre plusieurs domaines de traitement anti-spam.

**Projet de nouvelle Recommandation UIT-T X.1256 (X.authi), Lignes directrices et cadre pour le partage des résultats d'authentification réseau avec des applications de service****COM 17 – R 54**

**Résumé**

Du fait de l'augmentation rapide du nombre de dispositifs mobiles et d'applications permettant l'accès à Internet, l'environnement des services et du réseau devient de plus en plus compliqué. Il devient donc urgent de simplifier le mécanisme d'authentification de l'utilisateur, afin d'améliorer l'expérience de ce dernier et la qualité de service.

De nombreuses organisations de normalisation, parmi lesquelles l'UIT-T, ont accompli un important travail de recherche sur le mécanisme d'authentification unifié. Cependant, tous les travaux actuels se concentrent, dans l'ensemble, sur l'authentification unifiée pour plusieurs applications de services, sans tenir compte du lien existant avec l'authentification réseau.

Du point de vue de l'opérateur de réseau, l'utilisateur se soumet à certaines formes d'authentification réseau lorsqu'il se connecte à celui-ci, cette première authentification au réseau n'étant toutefois pas réutilisée lorsqu'il s'identifie ensuite à nouveau pour accéder à un service. L'adoption d'un mécanisme de partage des résultats d'authentification entre le service et le réseau permet d'identifier un utilisateur grâce aux résultats d'authentification fournis par le réseau. Un tel mécanisme permet à l'utilisateur de ne s'identifier qu'une seule fois par le biais du réseau et de pouvoir ensuite avoir directement accès au service souhaité.

La Recommandation UIT-T X.1256 présente des lignes directrices à l'intention des opérateurs de réseau et des fournisseurs de services pour le partage des résultats d'authentification réseau, et offre un cadre pour permettre le partage d'un nombre minimal d'attributs entre de multiples services, le tout dans une relation de confiance solide.

**Projet de nouvelle Recommandation UIT-T X.1257 (X.iamt), Taxonomie de la gestion d'identité
et d'accès****COM 17 – R 55**

**Résumé**

La Recommandation UIT-T X.1257 présente des spécifications dont le but est d'accorder l'importance nécessaire aux activités de gestion d'identité et d'accès, et de s'assurer de la traçabilité de ces activités tout au long du cycle de vie. Cela permettra d'attribuer efficacement les autorisations nécessaires aux utilisateurs, de réussir la mise en œuvre, dans différentes applications, des commandes de séparation des tâches, et de mener à bien les processus d'examen d'accès et de recoupement des données.

**Projet de Recommandation révisée UIT-T X.1521 (X.cvss), Système d'évaluation des vulnérabilités courantes 3.0****COM 17 – R 49**

**Résumé**

La Recommandation UIT-T X.1521 intitulée «Système d'évaluation des vulnérabilités courantes (CVSS)», qui 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. L'objectif de cette Recommandation 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'applications 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.1602 (X.sfcse), Exigences de sécurité pour l'environnement des applications de logiciel en tant que service (SaaS)****COM 17 – R 52**

**Résumé**

La Recommandation UIT-T X.1602 analyse le niveau de maturité des applications de logiciel en tant que service (SaaS) et propose la mise en place d'exigences de sécurité afin que l'exécution de ces applications se fasse dans un environnement cohérent et sûr. Des fournisseurs de services en nuage et des partenaires de services dans le nuage sont à l'initiative de ce projet, puisqu'ils doivent disposer d'un environnement pour les applications SaaS qui répond à leurs besoins en matière de sécurité. Ces exigences sont générales et indépendantes de tout modèle propre à un service, à un scénario particulier (comme les services web ou l'architecture REST), ou encore à des hypothèses ou solutions particulières.

**Projet de nouvelle Recommandation UIT-T X.1642 (X.goscc), Lignes directrices pour la sécurité opérationnelle de l'informatique en nuage****COM 17 – R 53**

**Résumé**

La Recommandation UIT-T X.1642 fournit des lignes directrices générales relatives à la sécurité opérationnelle pour l'informatique en nuage, du point de vue des fournisseurs de services en nuage. Cette Recommandation analyse les exigences de sécurité et les indicateurs pour le fonctionnement de l'informatique en nuage. Elle propose un ensemble de mesures et d'activités détaillées relatives à la sécurité pour le fonctionnement et la maintenance quotidiens de ces services, afin d'aider les fournisseurs à minimiser les risques relatifs à la sécurité et à résoudre les problèmes de sécurité liés au fonctionnement de l'informatique en nuage.

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