|  |  |
| --- | --- |
| **Oficina de Normalizaciónde las Telecomunicaciones** | **logo_S_** |
|  |  |

 Ginebra, 30 de septiembre de 2013

|  |  |  |
| --- | --- | --- |
| Ref.:Tel.:Fax: | **Circular TSB 52**COM 17/MEU+41 22 730 5866+41 22 730 5853 | - A las Administraciones de los Estados Miembros de la Unión |
| Correo-e: | tsbsg17@itu.int  | **Copia**:- A los Miembros del Sector UIT‑T;- A los Asociados del UIT‑T;- A las Instituciones Académicas del UIT-T;- Al Presidente y a los Vicepresidentes de laComisión de Estudio 17;- Al Director de la Oficina de Desarrollo de las Telecomunicaciones;- Al Director de la Oficina de Radiocomunicaciones |
|  |  |  |

|  |  |
| --- | --- |
| Asunto: | **Reunión de la Comisión de Estudio 17 para la aprobación de los proyectos de nuevas Recomendaciones UIT-T X.1210, X.1243 Cor.1, X.1546, X.1582 y X.1600 y de los proyectos de revisión de las Recomendaciones UIT-T X.1520 y X.1526 de conformidad con las disposiciones de la Resolución 1, Sección 9,de la AMNT (Dubai, 2012)Ginebra, 24 de enero de 2014** |

Muy Señora mía/Muy Señor mío:

1 A petición del Presidente de la Comisión de Estudio 17, *Seguridad*, tengo el honor de informarle que esta Comisión de Estudio, que se reunirá del 15 al 24 de enero de 2014, se propone aplicar el procedimiento descrito en la Resolución 1, Sección 9, de la AMNT (Dubai, 2012) para la aprobación de los proyectos de nuevas Recomendaciones y de corrigendum mencionados arriba.

2 El **anexo 1** contiene los títulos y resúmenes de los proyectos de nuevas Recomendaciones UIT‑T, con indicación de los documentos en que figuran.

3 Todo Estado Miembro, Miembro de Sector, Asociado o Institución Académica de la UIT consciente de la titularidad de una patente propia o ajena que pueda cubrir total o parcialmente los elementos de los proyectos de Recomendación propuestos para aprobación debe poner esa información en conocimiento de la TSB, de conformidad con la política sobre patentes del UIT‑T/UIT-R/ISO/CEI.

Puede accederse en línea a la información disponible sobre patentes a través del sitio web del UIT‑T ([www.itu.int/ITU-T/ipr/](http://www.itu.int/ITU-T/ipr/)).

4 Teniendo en cuenta las disposiciones de la Resolución 1, Sección 9, le agradecería que me comunicase **antes** de las 24.00 horas UTC **del 3 de enero de 2014** si su Administración otorga a la Comisión de Estudio 17 la autoridad necesaria para que durante su reunión pueda considerar la aprobación de estos proyectos de nuevas Recomendaciones y de corrigendum.

Si algunos Estados Miembros opinan que no puede procederse a considerar la aprobación, deben indicar sus razones de desaprobación así como los posibles cambios que facilitarían el nuevo examen y la aprobación de los proyectos de nuevas Recomendaciones y de corrigendum.

5 Si el 70% como mínimo de las respuestas de los Estados Miembros están a favor de que se considere la aprobación de estos proyectos de nueva Recomendación en la reunión de la Comisión de Estudio, **el 24 de enero de 2014** se dedicará una Sesión Plenaria a la aplicación del procedimiento de aprobación.

Invito pues a su Administración a que envíe un representante a dicha reunión. Se invita a las **Administraciones de los Estados Miembros de la Unión** a precisar el nombre de su Jefe de Delegación. Si su Administración desea estar representada en esa reunión por una empresa de explotación reconocida, un organismo científico o industrial u otra entidad que se ocupe de cuestiones de telecomunicaciones, habrá de comunicarlo al Director de conformidad con lo dispuesto en el Artículo 19, número 239, del Convenio de la UIT.

6 El orden del día y toda la información pertinente sobre la reunión de la Comisión de Estudio17 figurarán en la Carta Colectiva 3/17.

7 Después de la reunión, el Director de la TSB notificará por Circular la decisión tomada sobre estas Recomendaciones. Esta información se publicará también en el Boletín de Explotación de la UIT.

Le saluda muy atentamente.

Malcolm Johnson
Director de la Oficina de
Normalización de las Telecomunicaciones

**Anexo: 1**

ANEXO 1
(a la Circular TSB 52)

Resumen y ubicación de los textos

Proyecto de nueva Recomendación UIT-T X.1210 (X.trm), Aspectos generales de los mecanismos de detección del origen de los problemas de seguridad en las redes de protocolo Internet
COM 17 – R 12

Resumen

Para detectar el origen de los problemas de seguridad en las redes de protocolo Internet se emplean técnicas para obtener información técnica sobre los puntos de ingreso, los trayectos, los trayectos parciales u orígenes de un paquete o paquetes que causan problemas en la red, normalmente con el objetivo de solucionarlos.

En la Recomendación UIT-T X.1210 se presentan los aspectos generales de los mecanismos de detección del origen de los problemas de seguridad, además de los criterios de selección y las directrices de seguridad básica de esos mecanismos.

Proyecto de Corrigendum 1 de la Recomendación UIT-T X.1243, Sistema de pasarela interactiva para combatir el correo basura: Corrigendum 1
COM 17 – R 13

Resumen

Este Corrigendum 1 de la Recomendación UIT-T X.1243 (2010) corrige dos errores en la cláusula 7.2.7.

Proyecto de revisión de la Recomendación UIT-T X.1520 (X.cve), Vulnerabilidades y riesgos corrientes (CVE)
COM 17 – R 14

Resumen

En la Recomendación UIT-T X.1520 sobre la utilización de las vulnerabilidades y riesgos corrientes (CVE) se plantea un mecanismo estructurado para intercambiar vulnerabilidades y riesgos conocidos en materia de seguridad de la información destinado a proporcionar denominaciones comunes para los problemas conocidos públicamente que se plantean en los programas informáticos comerciales o de fuente abierta utilizados en las redes de comunicación, los dispositivos de usuario o cualquiera de los demás tipos de tecnologías de la información y la comunicación (TIC) aptos para utilizar programas informáticos. El objetivo de esta Recomendación es, gracias a esta denominación común, facilitar el intercambio de datos para distintos tipos de vulnerabilidad (herramientas, depósitos y servicios). La Recomendación está destinada a permitir la vinculación de bases de datos de vulnerabilidad y otras capacidades, y facilitar la comparación de las herramientas y servicios de seguridad. Como tal, CVE no recoge datos tales como el riesgo, las repercusiones, la información sobre la solución de problemas, o información técnica detallada. Sólo se recogen el número identificador habitual y el indicador de estado, una breve descripción, y referencias a los informes y consejos en materia de vulnerabilidad conexos. El registro de identificadores CVE puede consultarse en [cve.mitre.org/cve/cve.html].

CVE, cuya utilización se define en esta Recomendación, pretende ser exhaustivo en lo que respecta a todas las vulnerabilidades y los riesgos conocidos. Aunque se ha concebido para recoger información contrastada, su finalidad principal es la identificación de vulnerabilidades y riesgos que son detectados por las herramientas de seguridad y cualquier nuevo problema que se haga público, y en segundo lugar tratar cualquier problema de seguridad más antiguo que requiera validación.

Proyecto de revisión de la Recomendación UIT-T X.1526 (X.oval), Lenguaje abierto de vulnerabilidades y evaluación
COM 17 – R 15

Resumen

En la Recomendación UIT-T X.1526, Lenguaje abierto de vulnerabilidades y evaluación (OVAL), se normalizan las tres fases principales del proceso de evaluación: representación de la información de configuración de los puntos extremos en prueba; análisis del punto extremo para la detección de estados de máquina especificados (vulnerabilidad, configuración, parche, etc.) e información de los resultados de la evaluación. El objetivo de OVAL es ofrecer una norma comunitaria internacional sobre seguridad de la información para fomentar la disponibilidad pública y abierta de contenidos de seguridad y normalizar la transferencia de esta información a lo largo de todo el espectro de herramientas y servicios de seguridad. OVAL es un lenguaje utilizado para codificar los detalles de los puntos extremos, además de un conjunto de registros de contenido que mantiene la comunidad.

Proyecto de nueva Recomendación UIT-T X.1546 (X.maec), Enumeración y caracterización de atributos de malware
COM 17 – R 16

Resumen

El lenguaje de enumeración y caracterización de atributos de malware (software maligno) (MAEC)comprende enumeraciones de los atributos y comportamientos del malware con los que se forma un vocabulario común. Estas enumeraciones se sitúan a diversos niveles de abstracción: características observables de bajo nivel, comportamientos de nivel medio y taxonomías de alto nivel. La Recomendación UIT-T 1546, primera versión del MAEC, se centra en la creación de la enumeración de atributos de malware de bajo nivel basándose en los escasos trabajos sobre el tema ya existentes. Así, en un primer momento podrá caracterizar los tipos más comunes de malware, incluidos los troyanos, gusanos y *rootkits*, pero en último término podrá aplicarse a tipos más sofisticados de malware.

Proyecto de nueva Recomendación UIT-T X.1582 (X.cybex-tp), Protocolos de transporte para el intercambio de información de ciberseguridad
COM 17 – R 17

Resumen

En esta Recomendación se presentan los protocolos de transporte que se han adoptado para el intercambio de información de ciberseguridad (CYBEX) y que se han adaptado al mismo. Se describen las aplicaciones de transporte, las características de los protocolos de transporte y los aspectos relativos a la seguridad.

Proyecto de nueva Recomendación UIT-T X.1600 (X.ccsec), Marco de seguridad para la computación en la nube
COM 17 – R 19

Resumen

En la Recomendación UIT-T X.1600 se describe el marco de seguridad para la computación en la nube. En esta Recomendación se analizan las amenazas y problemas de seguridad en el entorno de la computación en la nube, y se describen las capacidades de seguridad que podrían contrarrestar las amenazas y solventar los problemas de seguridad. Se presenta una metodología marco para determinar qué capacidades de seguridad será necesario especificar para contrarrestar las amenazas de seguridad y solucionar los problemas de seguridad de la computación en la nube. En el Apéndice I se presenta un cuadro de correspondencia entre las amenazas y problemas de seguridad y la(s) capacidad(es) de seguridad que pueden eliminarlos.

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