Geneva, 30 September 2013

|  |  |
| --- | --- |
| **Telecommunication Standardization Bureau** |  |
|  |  |

|  |  |  |
| --- | --- | --- |
| Ref:  Tel:  Fax: | **TSB Circular 52**  COM 17/MEU  +41 22 730 5866 +41 22 730 5853 | - To Administrations of Member States of the Union |
| E-mail: | [tsbsg17@itu.int](mailto:tsbsg17@itu.int) | **Copy:**  - To ITU-T Sector Members;  - To ITU-T Associates;  - To ITU-T Academia;  - To the Chairman and Vice-Chairmen of Study Group 17;  - To the Director of the Telecommunication Development Bureau;  - To the Director of the Radiocommunication Bureau |

|  |  |
| --- | --- |
| Subject: | **Meeting of Study Group 17 with a view to approving draft new Recommendations ITU-T X.1210, X.1243 Cor.1, X.1546, X.1582 and X.1600 and draft revised Recommendations ITU-T X.1520 and X.1526 in accordance with the provisions of Resolution 1, Section 9, of WTSA (Dubai, 2012),  Geneva, 24 January 2014** |

Dear Sir/Madam,

1 At the request of the Chairman of Study Group 17, *Security*, I have the honour to inform you that this Study Group, which will meet from 15 to 24 January 2014, intends to apply the procedure described in Resolution 1, Section 9, of WTSA (Dubai, 2012) for the approval of the above-mentioned draft Recommendations and draft corrigendum.

2 The titles, summaries and location of the draft ITU-T Recommendations proposed for approval will be found in **Annex 1**.

3 Any ITU Member State, Sector Member, Associate or Academic Institution aware of a patent held by itself or others which may fully or partly cover elements of the draft Recommendations proposed for approval is requested to disclose such information to TSB, in accordance with the Common Patent Policy for ITU-T/ITU-R/ISO/IEC.

Available patent information can be accessed on‑line via the ITU‑T website ([www.itu.int/ITU-T/ipr/](http://www.itu.int/itu-t/ipr/)).

4 Having regard to the provisions of Resolution 1, Section 9, I should be grateful if you would inform me by 2400 hours UTC **on 3 January 2014** whether your Administration assigns authority to Study Group 17 that these draft Recommendations and corrigendum should be considered for approval at the Study Group meeting.

Should any Member States be of the opinion that consideration for approval should not proceed, they should advise their reasons for disapproving and indicate the possible changes that would facilitate further consideration and approval of the draft Recommendations and corrigendum.

5 If 70% or more of the replies from Member States support consideration for approval of these draft Recommendations and corrigendum at the Study Group meeting, one Plenary session will be devoted **on 24 January 2014** to apply the approval procedure.

I accordingly invite your Administration to send a representative to the meeting. **The Administrations of Member States of the Union** are invited to supply the name of the head of their delegation. If your Administration wishes to be represented at the meeting by a recognized operating agency, a scientific or industrial organization or another entity dealing with telecommunication matters, the Director should be duly informed, in accordance with Article 19, No. 239, of the ITU Convention.

6 The agenda and all relevant information concerning the Study Group 17 meeting will be available from Collective letter 3/17.

7 After the meeting, the Director of TSB will notify, in a circular, the decision taken on these Recommendations. This information will also be published in the ITU Operational Bulletin.

Yours faithfully,

Malcolm Johnson  
Director of the Telecommunication  
Standardization Bureau

**Annex: 1**

**ANNEX 1  
(to TSB Circular 52)**

**Summary and location of the texts**

**Draft new Recommendation ITU-T X.1210 (X.trm), Overview of source-based security troubleshooting mechanisms for Internet protocol-based networks  
COM 17 – R 12**

**Summary**

Source-based troubleshooting security issues in Internet protocol-based networks involve techniques used to discover technical information concerning the ingress points, paths, partial paths or sources of a packet or packets causing a problematic network event, generally for the purposes of applying mitigation measures.

Recommendation ITU-T X.1210 provides an overview of source-based security troubleshooting mechanisms for security issues, as well as selection criteria and basic security guidelines of troubleshooting mechanisms.

**Draft new Corrigendum 1 to Recommendation ITU-T X.1243, Interactive gateway system for countering spam: Corrigendum 1  
COM 17 – R 13**

**Summary**

This Corrigendum 1 to Recommendation ITU-T X.1243 (2010) corrects two errors in clause 7.2.7.

**Draft revised Recommendation ITU-T X.1520 (X.cve), Common vulnerabilities and exposures  
COM 17 – R 14**

**Summary**

Recommendation ITU-T X.1520 on the use of the common vulnerabilities and exposures (CVE) provides a structured means to exchange information security vulnerabilities and exposures that provides common names for publicly known problems in the commercial or open source software used in communications networks, end-user devices, or any of the other types of information and communications technology (ICT) capable of running software. The goal of the Recommendation is to define use of CVE to make it easier to share data across separate vulnerability capabilities (tools, repositories, and services) with this common naming. This Recommendation defines the use of CVE to provide a mechanism for vulnerability databases and other capabilities to be used together, and to facilitate the comparison of security tools and services. CVE does not contain information such as risk, impact, fix information, or detailed technical information. CVE only contains the standard identifier number with status indicator, a brief description, and references to related vulnerability reports and advisories. The repository of CVE identifiers is available at [cve.mitre.org/cve/cve.html].

The intention of CVE, the use of which is defined in this Recommendation, is to be comprehensive with respect to all publicly known vulnerabilities and exposures. While CVE is designed to contain mature information, the primary focus is on identifying vulnerabilities and exposures that are detected by security tools and any new problems that become public, and then addressing any older security problems that require validation.

**Draft revised Recommendation ITU-T X.1526 (X.oval), Open vulnerability and assessment language  
COM 17 – R 15**

**Summary**

In Recommendation ITU-T X.1526the Open Vulnerability and Assessment Language (OVAL)standardizes the three main steps of the assessment process: representing configuration information of endpoints for testing; analysing the endpoint for the presence of the specified machine state (vulnerability, configuration, patch state, etc.) and reporting the results of this assessment. The purpose of OVAL is to provide an international, information security, community standard to promote open and publicly available security content and to standardize the transfer of this information across the entire spectrum of security tools and services. OVAL is a language used to encode endpoint details, and an assortment of content repositories held throughout the community.

**Draft new Recommendation ITU-T X.1546 (X.maec), Malware attribute enumeration and characterization  
COM 17 – R 16**

**Summary**

The malware attribute enumeration and characterization (MAEC)language includes enumerations of malware attributes and behaviour that provide a common vocabulary. These enumerations are at different levels of abstraction: low-level observables, mid-level behaviours and high-level taxonomies. Recommendation ITU-T 1546, which is the initial version of MAEC, focuses on the creation of the enumeration of low-level malware attributes, and leverages the few instances of similar work already done in this area. Thus it will initially be capable of characterizing the most common malware types, including Trojans, worms, and rootkits, but will ultimately be applicable to more esoteric malware types.

**Draft new Recommendation ITU-T 1582 (X.cybex-tp), Transport protocols supporting cybersecurity information exchange  
COM 17 – R 17**

**Summary**

ThisRecommendation provides an overview of transport protocols that have been adopted and adapted for use within the Cybersecurity Information Exchange (CYBEX). The Recommendation outlines applications of transport, transport protocol characteristics, as well as security considerations.

**Draft new Recommendation ITU-T X.1600 (X.ccsec), Security framework for cloud computing  
COM 17 – R 19**

**Summary**

Recommendation ITU-T X.1600 describes the security framework for cloud computing. This Recommendation analyses security threats and challenges in the cloud computing environment, and describes security capabilities that could mitigate these threats and address security challenges. A framework methodology is provided for determining which of these security capabilities will require specification for mitigating security threats and addressing security challenges for cloud computing. Appendix I provides a mapping table on how a particular security threat or challenge is addressed by one or more corresponding security capabilities.

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