|  |  |
| --- | --- |
| **مكتب تقييس الاتصالات** | logo_A-[Converted] |

|  |  |  |
| --- | --- | --- |
|  |  | جنيف، 30 سبتمبر 2013 |
| المرجع: | **TSB Circular 52**COM 17/MEU | - إلى إدارات الدول الأعضاء في الاتحاد |
| الهاتف:الفاكس:البريد الإلكتروني: | +41 22 730 5866+41 22 730 5853tsbsg17@itu.int | **نسخة إلى:**- أعضاء قطاع تقييس الاتصالات؛- المنتسبين إلى قطاع تقييس الاتصالات؛- الهيئات الأكاديمية المنضمة إلى قطاع تقييس الاتصالات؛- رئيس لجنة الدراسات 17 ونوابه؛- مدير مكتب تنمية الاتصالات؛- مدير مكتب الاتصالات الراديوية |
|  |  |  |
| الموضوع: | **اجتماع ل‍جنة الدراسات 17 بهدف ال‍موافقة على مشاريع التوصيات ال‍جديدة ITU‑T X.1210 وX.1243 (التصويب (1، وX.1546 وX.1582 وX.1600 ومشروعي مراجعة التوصيتين ITU‑T X.1520 وX.1526 عملاً بأحكام القسم 9 من القرار 1 الصادر عن ال‍جمعية العال‍مية لتقييس الاتصالات (دبي، 2012)، جنيف، 24 يناير 2014** |

حضرات السادة والسيدات،

ت‍حية طيبة وبعد،

1 بناءً على طلب رئيس ل‍جنة الدراسات 17 ال‍معنية ب‍موضوع *الأمن*، أتشرف بأن أعلمكم أن ل‍جنة الدراسات هذه، التي ستجتمع من 15 إلى 24 يناير 2014، تنوي تطبيق الإجراءات ال‍موصوفة في القسم 9 من القرار 1 الصادر عن ال‍جمعية العالمية لتقييس الاتصالات (دبي، 2012) وذلك من أجل ال‍موافقة على مشاريع التوصيات ال‍مشار إليها أعلاه ب‍ما في ذلك مشروع تصويب.

2 ويشتمل **ال‍ملحق 1** بهذه الرسالة على عناوين مشاريع توصيات قطاع تقييس الاتصالات ال‍مقترح الموافقة عليها، وعلى ملخصاتها والوثائق التي يرد فيها مشروع كل توصية.

3 يرجى من أي دولة عضو في الات‍حاد أو عضو في القطاع أو منتسب إليه أو مؤسسة أكادي‍مية تعلم بوجود براءة اختراع في حيازته أو في حيازة الغير من شأنها أن تشمل كلياً أو جزئياً عناصر من مشاريع التوصيات ال‍مقترح ال‍موافقة عليها أن يُفصح عن هذه ال‍معلومات ل‍مكتب تقييس الاتصالات، عملاً بالسياسة ال‍مشتركة للبراءات ال‍معتمدة لدى قطاع تقييس الاتصالات/قطاع الاتصالات الراديوية/ال‍منظمة الدولية للتوحيد القياسي/اللجنة الكهرتقنية الدولية (ITU‑T/ITU‑R/ISO/IEC).

وي‍مكن الاطلاع على معلومات براءات الاختراع ال‍متاحة في ال‍موقع الإلكتروني للقطاع ([www.itu.int/ITU-T/ipr/](http://www.itu.int/itu-t/ipr/)).

4 وتبعاً لأحكام القسم 9 من القرار 1 سأكون م‍متناً لو تفضلتم بإعلامي في موعد أقصاه منتصف الليل بالتوقيت العال‍مي ال‍منسَّق **في 3 يناير 2014** ما إذا كانت إدارتكم تفوِّض السلطة إلى ل‍جنة الدراسات 17 للنظر في مشاريع التوصيات والتصويب بغرض الموافقة عليها في اجتماع ل‍جنة الدراسات.

وإذا رأت أي دولة عضو أن عملية النظر بغرض ال‍موافقة ينبغي ألاّ تستمر فعليها أن تبيّن أسباب ذلك الاعتراض وأن تشير إلى التغييرات ال‍ممكنة التي من شأنها تيسير مواصلة النظر في مشاريع التوصيات والتصويب وال‍موافقة عليها.

5 فإذا كان 70 في ال‍مائة أو أكثر من الردود الواردة من الدول الأعضاء تؤيد النظر في مشاريع التوصيات والتصويب بغرض ال‍موافقة عليها في اجتماع ل‍جنة الدراسات، عندئذ سوف تُكرَّس جلسة عامة **في 24 يناير 2014** لتطبيق إجراءات ال‍موافقة.

ولذلك فإنني أدعو إدارتكم إلى إيفاد م‍مثل إلى الاجتماع. **ويرجى من إدارات الدول الأعضاء في الات‍حاد** بيان اسم رئيس وفدها. وإذا كانت إدارتكم ترغب في أن ي‍مثلها في الاجتماع وكالة تشغيل معتمدة أو منظمة علمية أو صناعية أو أي كيان آخر يتعامل في مسائل الاتصالات، ينبغي إبلاغ ال‍مدير بذلك طبقاً لأحكام الرقم 239 من ال‍مادة 19 من اتفاقية الات‍حاد.

6 وي‍مكن الاطلاع على جدول الأعمال وج‍ميع ال‍معلومات ذات الصلة فيما يتعلق باجتماع ل‍جنة الدراسات 17 في الرسالة ال‍جماعية 3/17.

7 وفي أعقاب الاجتماع سوف يعلن مدير مكتب تقييس الاتصالات، في رسالة معممة، عن القرار ال‍مُتَخّذ بشأن هذه التوصيات. وسوف تُنشر هذه المعلومات أيضاً في النشرة التشغيلية للات‍حاد.

وتفضلوا بقبول فائق التقدير والاحترام.

مالكولم جونسون
مدير مكتب تقييس الاتصالات

**ال‍ملحقات: 1**

ال‍ملحـق 1
(بالرسالة ال‍معممة 52 ل‍مكتب تقييس الاتصالات)

ملخص النصوص والوثائق التي ترد فيها

مشروع التوصية ال‍جديدة ITU-T X.1210 (X.trm)، ل‍محة عامة عن آليات حل ال‍مشاكل الأمنية القائمة على ال‍مصدر في الشبكات القائمة على بروتوكول الإنترنت
COM 17 - R 12

ملخص

تشمل آليات حل المشاكل الأمنية على أساس المصدر في الشبكات القائمة على بروتوكول الإنترنت تقنيات تُستعمل لكشف المعلومات التقنية المتعلقة بنقاط الدخول وال‍مسيرات وال‍مسيرات ال‍جزئية أو مصادر الرزمة أو الرزم المسببة للمشاكل في الشبكات، وذلك لأغراض تطبيق تدابير التخفيف عموماً.

وتقدم التوصية ITU-T X.1210 ل‍محة عامة عن آليات حل المشاكل الأمنية القائمة على المصدر من أجل المسائل المتعلقة بالأمن، فضلاً عن معايير الاختيار والمبادئ التوجيهية الأمنية الأساسية لآليات حل المشاكل.

مشروع التصويب 1 ال‍جديد للتوصية ITU-T X.1243، نظام البوابة التفاعلية ل‍مكافحة الرسائل الاقتحامية: التصويب 1
COM 17 - R 13

ملخص

الغرض من التصويب 1 للتوصية ITU-T X.1243 (2010) تصويب خطأين في البند 7.2.7.

مشروع مراجعة التوصية ITU-T X.1520 (X.cve)، مواطن الضعف والتعرض الشائعة (CVE)
COM 17 - R 14

ملخص

تتناول التوصية ITU-T X.1520 بشأن استعمال مواطن الضعف والتعرض الشائعة (CVE) وسائل منظمة لتبادل معلومات الأمن بشأن مواطن الضعف والتعرض الشائعة من أجل توفير تسميات مشتركة للمشاكل المعروفة في البرمجيات التجارية أو مفتوحة المصدر المستعملة في شبكات الاتصالات، وأجهزة المستعمل النهائي أو أي نمط آخر من أنماط تكنولوجيا المعلومات والاتصالات القادرة على تشغيل البرمجيات. والهدف من هذه التوصية تعريف مواطن الضعف والتعرض الشائعة لتيسير تقاسم البيانات عبر قدرات منفصلة لتحديد مواطن الضعف (أدوات وسجلات وخدمات) باستعمال هذه التسميات المشتركة. وتعرّف هذه التوصية استعمال مواطن الضعف والتعرض لتوفير آليات تسمح باستعمال قواعد بيانات مواطن الضعف والقدرات الأخرى مع بعضها البعض، وتسهيل مقارنة الأدوات والخدمات الأمنية. ولا تتضمن مواطن الضعف والتعرض معلومات بشأن المخاطر أو الآثار أو معلومات لحل المشاكل أو معلومات تقنية مفصلة. فهي تتضمن فقط رقم معرف الهوية المعياري ومؤشر الحالة ووصفاً موجزاً وإحالات إلى تقارير وإرشادات متصلة ب‍مواطن الضعف. وسجل معرفات هوية مواطن الضعف والتعرض متاح في الموقع [cve.mitre.org/cve/cve.html].

والغرض من مواطن الضعف والتعرض، المعرّف استعمالها في هذه التوصية، أن تكون شاملة فيما يتعلق بجميع مواطن الضعف والتعرض المعروفة. وعلى الرغم من أنها أعدت لتشمل معلومات وافية، فإن التركيز الأول ينصب على تحديد مواطن الضعف والتعرض التي يتم كشفها بواسطة أدوات الأمن وأي مشاكل جديدة تصبح شائعة، ثم معالجة أي مشاكل أمنية قديمة تقتضي التحقق.

مشروع مراجعة التوصية ITU-T X.1526 (X.oval)، لغة التقييم والتعرض ال‍مفتوحة
COM 17 – R 15

ملخص

تقوم لغة التقييم والتعرض المفتوحة (OVAL) الواردة في التوصية ITU-T X.1526 بتقييس الخطوات الرئيسية الثلاث لعملية التقييم، وهي: ت‍مثيل معلومات تشكيل النقاط الطرفية لأغراض الاختبار؛ وتحليل النقاط الطرفية بحثاً عن وجود حالة موصَّفة للآلة (نقطة ضعف، أو تشكيل، أو حالة رقعة برمجية، وما إلى ذلك)؛ والإبلاغ عن نتائج هذا التقييم. والغرض من اللغة OVAL توفير معيار دولي لمجتمع أمن المعلومات من أجل النهوض بمحتوى أمني مفتوح ومتاح للجمهور وتقييس نقل هذه المعلومات عبر كل أنواع أدوات الأمن وخدماته. وتُستخدم اللغة OVAL لتشفير تفاصيل النقاط الطرفية ومجموعة متنوعة من سجلات المحتويات القائمة في جميع أنحاء مجتمع أمن المعلومات.

مشروع التوصية ال‍جديدة ITU-T X.1546 (X.maec)، تعداد نعوت البرم‍جيات ال‍خبيثة وت‍حديد خصائصها
COM 17 – R 16

ملخص

تشمل لغة تعداد نعوت البرمجيات الخبيثة وتحديد خصائصها (MAEC) تعدادات نعوت البرمجيات الخبيثة وسلوكها التي توفر مصطلحات شائعة. وتتم هذه التعدادات على مستويات تجريد مختلفة: الخاصيات القابلة للرصد منخفضة المستوى والسلوكيات متوسطة المستوى والتصنيفات رفيعة المستوى. وتركز التوصية ITU-T X.1546 التي هي النسخة الأولية للغة MAEC، على استحداث نظام تعداد نعوت البرمجيات الخبيثة منخفضة المستوى والاستفادة من الحالات القليلة للأعمال الشبيهة المنجزة فعلاً في هذا المجال. وبالتالي فهي قادرة أولاً على تحديد خصائص أكثر أنواع البرمجيات الخبيثة شيوعاً بما في ذلك برمجيات أحصنة طروادة والديدان والحزم الجذرية، ولكن يمكن تطبيقها في نهاية الأمر على أنواع أكثر تخفياً من البرمجيات الخبيثة.

مشروع التوصية ال‍جديدة ITU-T X.1582 (X.cybex-tp)، بروتوكولات النقل ال‍مستعملة لدعم تبادل معلومات الأمن السيبراني
COM 17 – R 17

ملخص

تقدم هذه التوصية ل‍محة عامة عن بروتكولات النقل التي تم اعتمادها وتكييفها لاستعمالها في إطار تبادل معلومات الأمن السيبراني (CYBEX). وتلخص هذه التوصية تطبيقات النقل وخصائص بروتوكول النقل فضلاً عن الاعتبارات الأمنية.

مشروع التوصية ال‍جديدة ITU-T X.1600 (X.ccses)، إطار أمني للحوسبة السحابية
COM 17 – R 19

ملخص

تصف التوصية ITU-T X.1600 الإطار الأمني للحوسبة السحابية. وتقوم بتحليل التهديدات والتحديات الأمنية في بيئة الحوسبة السحابية، وتصف القدرات الأمنية التي من شأنها التخفيف من هذه التهديدات والتصدي للتحديات الأمنية. وتُقدم منهجية إطارية لتحديد القدرات الأمنية التي ستتطلب وضع مواصفات للتخفيف من التهديدات الأمنية والتصدي للتحديات الأمنية في الحوسبة السحابية. ويقدم التذييل الأول جدول تقابل بشأن كيفية التصدي لتهديد أو تحدٍ أمني معين باستخدام قدرة واحدة أو أكثر من القدرات الأمنية المقابلة.

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