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

|  |  |  |
| --- | --- | --- |
|  |  | جنيف، 6 مارس 2012 |
| المرجع: | **TSB Circular 266** COM 17/MEU | * إلى إدارات الدول الأعضاء في الاتحاد |
| الهاتف: الفاكس: البريد الإلكتروني: | +41 22 730 5866 +41 22 730 5853[tsbsg17@itu.int](mailto:tsbsg17@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: | **الموافقة على المسألة 8/17 المراجعة** | |

حضرات السادة والسيدات،

تحية طيبة وبعد،

1 بناءً على طلب رئيس لجنة الدراسات 17، *الأمـن*، أتشرف بإبلاغكم بأن الدول الأعضاء وأعضاء القطاع الحاضرين في الاجتماع الأخير للجنة الدراسات، الذي عقد في جنيف في الفترة من 20 فبراير إلى 2 مارس 2012، اتفقوا، بتوافق الآراء، وفقاً للإجراء المبين في الفقرة 2.2.7 من القسم 7 من القرار 1 للجمعية العالمية لتقييس الاتصالات (جوهانسبرغ، 2008)، على الموافقة على المسألة المراجعة التالية:

*المسألة 8/17، أمن الحوسبة السحابية* (انظر الملحق 1)

2 **ومن ثمَّ، تمت الموافقة على المسألة 8/17.**

3 ومن المفترض أن تخضع التوصيات الناجمة عن ذلك لعملية الموافقة التقليدية (TAP).

وتفضلوا بقبول فائق التقدير والاحترام.

مالكولم جونسون  
مدير مكتب تقييس الاتصالات

**الملحقات:** 1

**الملحـق 1**  
(بنشرة مكتب تقييس الاتصالات رقم 266)

المسألة 8/17، أمن الحوسبة السحابية

(مسألة مراجعة)

# الدوافع

الحوسبة السحابية عبارة عن نموذج لتمكين مستعمل الشبكة من النفاذ الشبكي من كل مكان وفي أي وقت بسهولة وعند الحاجة إلى مجموعة مشتركة من موارد الحوسبة القابلة للتشكيل (مثل، الشبكات والمخدمات والتخزين والتطبيقات والخدمات)، التي يمكن توفيرها وتسليمها بسرعة مع أدنى حد من الجهد الإداري أو التدخل من جانب مورد الخدمة. ويتألف نموذج الحوسبة السحابية من خمسة خصائص أساسية (الخدمة بناءً على الطلب، والتسليم عبر نفاذ شبكي واسع وتجميع الموارد وسرعة المرونة والخدمات الذاتية والمقيسة)، وخمس فئات لخدمة الحوسبة السحابية أي البرمجيات كخدمة (SaaS) والاتصال كخدمة (CaaS) والمنصات كخدمة (PaaS) والبنية التحتية كخدمة (IaaS) والشبكات كخدمة (NaaS) ونماذج النشر المختلفة (العامة والخاصة والهجينة ...). وأدى ظهور نهج الحوسبة السحابية بوصفه الأداة المفضلة للاكتشاف وإخراج البيانات والتركيب وإعادة استعمال الخدمة في إطار سير العمل والتطبيقات والتطبيقات المدعومة بالاتصالات، إلى التأكيد من جديد على الحاجة إلى الأمن.

وتشمل الفوائد المتوقعة من الحوسبة السحابية توفير موارد مرنة ودينامية وإدارة أكثر بساطة وتلقائية للبنية التحتية لتكنولوجيا المعلومات. وتمكن التقنية الافتراضية من تقاسم موارد غير محدودة تقريباً، مع إدخال تحسينات تتعلق بالمرونة وإجراء تخفيض هائل في تكاليف إدارة البنية التحتية. ومع ذلك، تثير الأنظمة المفتوحة وتقاسم الموارد في إطار نظام الحوسبة السحابية العديد من المخاوف المتعلقة بالأمن وربما كان ذلك أهم حاجز يحول دون اعتماد الحوسبة السحابية. فالانتقال إلى الحوسبة السحابية ينطوي على التحول من أنظمة تكنولوجيا المعلومات التقليدية الداخلية والآمنة إلى بنى تحتية مفتوحة وغير آمنة وقائمة على تكنولوجيا الحوسبة السحابية. وبالتالي فإنه يتطلب إعادة التفكير المتعمق في مسألة الأمن.

واعتبرت الحوسبة السحابية لعدة سنوات تكنولوجيا المعلومات التي تركز على الخدمة وتسيطر عليها الجهات الفاعلة المعنية بشبكة الإنترنت. ومع ذلك، بإمكان الجهات الفاعلة في مجال الاتصالات أداء دور هام في سوق الحوسبة السحابية الناشئة وبيئتها. وبما أن الخدمات السحابية تتاح من خلال شبكات الاتصالات، ينبغي على الجهات الفاعلة في مجال الاتصالات كفالة مستوى عال من الضمان. ومن شأن إتاحة حماية قوية ولكنها مرنة أن تكون داعماً رئيسياً لمجمل سوق الحوسبة السحابية وبيئتها.

وبالإضافة إلى ذلك، فإن المرونة في استخدام الموارد الغنية في بيئات الحوسبة السحابية سوف تمكن من إتاحة خدمات أمنية جديدة لا يمكن لآليات الدفاع الحالية المتاحة في المقر توفيرها (خدمات مكافحة البرمجيات الخبيثة كخدمة سحابية، على سبيل المثال). وبالتالي، هناك حاجة إلى دراسة ما يمكن للحوسبة السحابية أن تقدمه من أنواع التدابير الأمنية في المستقبل القريب.

وتتيح مشاريع التوصيات ITU‑T X.ccsec وITU‑T X.srfcts وITU‑T X.sfcse لقطاع تقييس الاتصالات، تقديم مجموعة من التوصيات بشأن الخدمات الأمنية لإتاحة خدمات تتعلق بالوضع العام لأمن الحوسبة السحابية والمعمارية والإطار وأمن الحوسبة السحابية عبر الطبقات وأمن خدمات الشبكات خصوصاً. وحالياً توجد حاجة ماسة لتأمين الخدمات التي تدعمها الحوسبة السحابية ومنها خدمات الصوت والوسائط المتعددة والخدمات القائمة على الهوية وخدمات ضمان المعلومات وخدمات الهوية والبيانات والخدمات في حالات الطوارئ. وتهدف هذه المسألة إلى بلورة توصيات جديدة تستند إلى الجزء 5 من التقرير التقني للفريق المتخصص المعني بالحوسبة السحابية من أجل ما يلي:

• وضع أفضل الممارسات والمبادئ التوجيهية للاسترشاد بها في كيفية توفير الأمن في بيئة قائمة على الحوسبة السحابية؛

• توضيح المسؤولية وتعريف متطلبات الأمن وتحديد التهديدات الأمنية لفائدة الجهات الفاعلة الرئيسية وأدوارها ذات الصلة في بيئة الحوسبة السحابية؛

• بنية أمنية قائمة على أساس المعمارية المرجعية الواردة في المسألة 27/13؛

• إدارة الأمن وتكنولوجيا التدقيق من أجل إدارة المسائل المتعلقة بالثقة.

وسوف تتعاون المسألة 8/17 مع المسائل ذات الصلة مثل 2/17 و3/17 و4/17 و7/17 و10/17 و11/17 لوضع توصيات بشأن أمن الحوسبة السحابية.

وتشمل التوصيات والإضافات الواقعة تحت مسؤولية هذه المسألة اعتباراً من 2 مارس 2012: ITU‑T X.ccsec وITU‑T X.sfcse وITU‑T X.fssvpn لقطاع تقييس الاتصالات.

# المسألة

تشمل بنود الدراسة التي سينظر فيها، على سبيل المثال لا الحصر، ما يلي:

أ ) ما هي التوصيات الجديدة أو الأنواع الأخرى من الوثائق التي ينبغي وضعها لتستفيد منها الجهات الفاعلة الرئيسية مثل مقدمي الخدمات ومستخدمي الخدمات والشركاء في الخدمات وغيرهم من أصحاب المصلحة الرئيسية في دوائر الصناعة لتعزيز أمن الحوسبة السحابية؟

ب) ما هي التوصيات الجديدة التي ينبغي وضعها بشأن معمارية الأمن وتنظيم الوظائف الأمنية وفقاً للمعمارية المرجعية؟

ج) ما هي التوصيات الجديدة التي ينبغي وضعها بشأن إدارة الأمن وآليات الضمان وتكنولوجيات التدقيق وما يرتبط بها من تقدير المخاطر لبناء الثقة بين مختلف الجهات الفاعلة؟

د ) ما هو مجال التعاون اللازم للحد من ازدواجية الجهود مع المسائل الأخرى ولجان الدراسات ومنظمات وضع المعايير، تحت رعاية نشاط التنسيق المشترك المعني بالحوسبة السحابية؟

ﻫ ) كيف ينبغي تطوير الأمن كخدمة لحماية أنظمة تكنولوجيا المعلومات والاتصالات؟

# المهـام

تشمل المهام على سبيل المثال لا الحصر، ما يلي:

أ ) وضع توصيات أو أي نوع آخر من الوثائق لتعزيز أمن الحوسبة السحابية.

ب) وضع توصيات لتحديد المتطلبات الأمنية والتهديدات الأمنية من أجل تأمين خدمات الحوسبة السحابية على أساس المتطلبات العامة للحوسبة السحابية التي تحددها لجنة الدراسات 13 لقطاع تقييس الاتصالات.

ج) وضع توصيات لتحديد معمارية إدارة الأمن وتنظيم الوظائف الأمنية على أساس المعمارية المرجعية التي تحددها لجنة الدراسات 13 لقطاع تقييس الاتصالات.

د ) وضع توصيات لتحديد معمارية قوية ومرنة لإدارة الأمن وتنفيذه لأنظمة الحوسبة السحابية.

ﻫ ) وضع توصيات لتحديد آليات الضمان وتكنولوجيات التدقيق وتقييم المخاطر وذلك بهدف التوصل إلى إقامة علاقات ثقة داخل بيئة الحوسبة السحابية.

و ) الاضطلاع بجميع الأنشطة المتعلقة بأمن الحوسبة السحابية في إطار لجنة الدراسات 17.

ز ) تمثيل لجنة الدراسات 17 فيما يتعلق بعملها المعني بأمن الحوسبة السحابية، في إطار نشاط التنسيق المشترك المعني بالحوسبة السحابية.

# الروابط

التوصيات:

• توصيات السلسلة Y بشأن الحوسبة السحابية

المسائل:

• المسائل 1/17 و2/17 و3/17 و4/17 و7/17 و10/17 و11/17 لقطاع تقييس الاتصالات

لجان الدراسات:

• لجان الدراسات 2 و13 و16 لقطاع تقييس الاتصالات

هيئات التقييس:

• اللجنتان الفرعيتان 27 و38 التابعتان للجنة التقنية المشتركة الأولى للمنظمة الدولية للتوحيد القياسي واللجنة الكهرتقنية الدولية (ISO/IEC JTC 1)؛ ومنظمة تطوير معايير المعلومات المنسقة (OASIS)؛ وفريق مهام هندسة الإنترنت (IETF) وغيرها من الهيئات المعنية التي يجري تحديدها.

هيئات أخرى:

• فريق مهام إدارة سطح المكتب؛ والتحالف المعني بأمن الحوسبة السحابية (CSA).

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