الاتحـــــــــاد الدولـــــــــي للاتصـــــــــالات

ITU-T

قطاع تقييس الاتصالات
في الاتحاد الدولي للاتصالات

X.1606

(2020/09)

السلسلة X: شبكات البيانات والاتصالات بين الأنظمة المفتوحة ومسائل الأمن

أمن الحوسبة السحابية – تصميم أمن الحوسبة السحابية

المتطلبات الأمنية لبيئات تطبيقات "الاتصالات كخدمة"

التوصية ITU-T X.1606

الاتحاد الدولي للاتصالات

توصيات السلسلة X الصادرة عن قطاع تقييس الاتصالات

شبكات البيانات والاتصالات بين الأنظمة المفتوحة ومسائل الأمن

الشبكات العمومية للبيانات	X.199–X.1
التوصيل البيني للأنظمة المفتوحة	X.299–X.200
التشغيل البيني للشبكات	X.399–X.300
أنظمة معالجة الرسائل	X.499–X.400
الدليل	X.599–X.500
التشغيل البيني لأنظمة التوصيل OSI ومظاهر النظام	X.699–X.600
إدارة التوصيل البيني للأنظمة المفتوحة (OSI)	X.799–X.700
الأمن	X.849–X.800
تطبيقات التوصيل البيني للأنظمة المفتوحة (OSI)	X.899–X.850
المعالجة الموزعة المفتوحة	X.999–X.900
أمن المعلومات والشبكات	
الجوانب العامة للأمن	X.1029–X.1000
أمن الشبكة	X.1049–X.1030
إدارة الأمن	X.1069–X.1050
الخصائص البيومترية	X.1099–X.1080
تطبيقات وخدمات آمنة (1)	
أمن البث المتعدد	X.1109–X.1100
أمن الشبكة المحلية	X.1119–X.1110
أمن الخدمات المتنقلة	X.1139–X.1120
أمن الويب	X.1149–X.1140
بروتوكولات الأمن (1)	X.1159–X.1150
الأمن بين جهتين نظيرتين	X.1169–X.1160
أمن معرفات الهوية عبر الشبكات	X.1179–X.1170
أمن التلفزيون القائم على بروتوكول الإنترنت	X.1199–X.1180
أمن الفضاء السيبراني	
الأمن السيبراني	X.1229–X.1200
مكافحة الرسائل الاقتحامية	X.1249–X.1230
إدارة الهوية	X.1279–X.1250
تطبيقات وخدمات آمنة (2)	
اتصالات الطوارئ	X.1309–X.1300
أمن شبكات المحاسيس واسعة الانتشار	X.1319–X.1310
أمن شبكة الكهرباء الذكية	X.1339–X.1330
البريد المعتمد	X.1349–X.1340
أمن إنترنت الأشياء (IoT)	X.1369–X.1360
أمن أنظمة النقل الذكية (ITS)	X.1389–X.1370
أمن سجل الحسابات الموزع	X.1429–X.1400
أمن سجل الحسابات الموزع	X.1449–X.1430
البروتوكول الأمني (2)	X.1459–X.1450
تبادل معلومات الأمن السيبراني	
نظرة عامة عن الأمن السيبراني	X.1519–X.1500
تبادل مواطن الضعف/الحالة	X.1539–X.1520
تبادل الأحداث/الأحداث العارضة/المعلومات الحدسية	X.1549–X.1540
تبادل السياسات	X.1559–X.1550
طلب المعلومات الحدسية والمعلومات الأخرى	X.1569–X.1560
تعرف الهوية والاكتشاف	X.1579–X.1570
التبادل المضمون	X.1589–X.1580
أمن الحوسبة السحابية	
نظرة عامة على أمن الحوسبة السحابية	X.1601–X.1600
تصميم أمن الحوسبة السحابية	**X.1639–X.1602**
أفضل الممارسات ومبادئ توجيهية بشأن أمن الحوسبة السحابية	X.1659–X.1640
تنفيذ أمن الحوسبة السحابية	X.1679–X.1660
أمن أشكال أخرى للحوسبة السحابية	X.1699–X.1680
الاتصالات الكمومية	
المصطلحات	X.1701–X.1700
مولّد الأعداد العشوائية الكمومية	X.1709–X.1702
إطار أمن شبكات توزيع المفاتيح الكمومية	X.1711–X.1710
تصميم أمن شبكات توزيع المفاتيح الكمومية	X.1719–X.1712
تقنيات أمن شبكات توزيع المفاتيح الكمومية	X.1729–X.1720
أمن البيانات	
أمن البيانات الضخمة	X.1759–X.1750
أمن شبكات الجيل الخامس	X.1819–X.1800

لمزيد من التفاصيل يرجى الرجوع إلى قائمة التوصيات الصادرة عن قطاع تقييس الاتصالات.

التوصية ITU-T X.1606

المتطلبات الأمنية لبيئات تطبيقات 'الاتصالات كخدمة'

ملخص

تحدد التوصية ITU-T X.1606 التهديدات الأمنية التي قد تتعرض لها بيئات تطبيقات 'الاتصالات كخدمة' (CaaS) وتوصي بالمتطلبات الأمنية اللازمة للتصدي لهذه التهديدات. وتبين هذه التوصية سيناريوهات وسمات 'الاتصالات كخدمة' الشاملة لقدرات اتصالات متعددة، ثم تحدد التهديدات الأمنية الناشئة عن هذه السمات الفريدة وتوصي بالمتطلبات الأمنية اللازمة للتصدي لهذه التهديدات.

التسلسل التاريخي

الطبعة	التوصية	تاريخ الموافقة	لجنة الدراسات	معرف الهوية الفريد*
1.0	ITU-T X.1606	2020-09-03	17	11.1002/1000/14265

مصطلحات أساسية

الاتصالات كخدمة، حوسبة سحابية، مخاطر، متطلبات أمنية.

* للنفاذ إلى توصية، ترجى كتابة العنوان http://handle.itu.int/ في حقل العنوان في متصفح الويب لديكم، متبوعاً بمعرف التوصية الفريد. ومثال ذلك، http://handle.itu.int/11.1002/1000/11830-en.

تمهيد

الاتحاد الدولي للاتصالات وكالة متخصصة للأمم المتحدة في ميدان الاتصالات وتكنولوجيات المعلومات والاتصالات (ICT). وقطاع تقييس الاتصالات (ITU-T) هو هيئة دائمة في الاتحاد الدولي للاتصالات. وهو مسؤول عن دراسة المسائل التقنية والمسائل المتعلقة بالتشغيل والتعريفة، وإصدار التوصيات بشأنها بغرض تقييس الاتصالات على الصعيد العالمي.

وتحدد الجمعية العالمية لتقييس الاتصالات (WTSA) التي تجتمع مرة كل أربع سنوات المواضيع التي يجب أن تدرسها لجان الدراسات التابعة لقطاع تقييس الاتصالات وأن تُصدر توصيات بشأنها.

وتتم الموافقة على هذه التوصيات وفقاً للإجراء الموضح في القرار 1 الصادر عن الجمعية العالمية لتقييس الاتصالات.

وفي بعض مجالات تكنولوجيا المعلومات التي تقع ضمن اختصاص قطاع تقييس الاتصالات، تُعد المعايير اللازمة على أساس التعاون مع المنظمة الدولية للتوحيد القياسي (ISO) واللجنة الكهرتقنية الدولية (IEC).

ملاحظة

تستخدم كلمة "الإدارة" في هذه التوصية لتدل بصورة موجزة سواء على إدارة اتصالات أو على وكالة تشغيل معترف بها.

والتقيد بهذه التوصية اختياري. غير أنها قد تضم بعض الأحكام الإلزامية (بهدف تأمين قابلية التشغيل البيني والتطبيق مثلاً). ويعتبر التقيّد بهذه التوصية حاصلاً عندما يتم التقيّد بجميع هذه الأحكام الإلزامية. ويستخدم فعل "يلزم" وصيغ ملزمة أخرى مثل فعل "يجب" وصيغها النافية للتعبير عن متطلبات معينة، ولا يعني استعمال هذه الصيغ أن التقيّد بهذه التوصية إلزامي.

حقوق الملكية الفكرية

يسترعي الاتحاد الانتباه إلى أن تطبيق هذه التوصية أو تنفيذها قد يستلزم استعمال حق من حقوق الملكية الفكرية. ولا يتخذ الاتحاد أي موقف من القرائن المتعلقة بحقوق الملكية الفكرية أو صلاحيتها أو نطاق تطبيقها سواء طالب بها عضو من أعضاء الاتحاد أو طرف آخر لا تشمله عملية إعداد التوصيات.

وعند الموافقة على هذه التوصية، لم يكن الاتحاد قد تلقى إخطاراً بملكية فكرية تحميها براءات الاختراع يمكن المطالبة بها لتنفيذ هذه التوصية. ومع ذلك، ونظراً إلى أن هذه المعلومات قد لا تكون هي الأحدث، يوصى المسؤولون عن تنفيذ هذه التوصية بالاطلاع على قاعدة البيانات الخاصة ببراءات الاختراع في مكتب تقييس الاتصالات (TSB) في الموقع http://www.itu.int/ITU-T/ipr/.

جدول المحتويات

الصفحة

التوصية ITU-T X.1606

المتطلبات الأمنية لبيئات تطبيقات 'الاتصالات كخدمة'

1 مجال التطبيق

تركز هذه التوصية على المتطلبات الأمنية لبيئات تطبيقات 'الاتصالات كخدمة' (CaaS)، المختلفة عن بيئات تطبيقات 'البرمجيات كخدمة' (SaaS) المبيّنة في التوصية [ITU-T X.1602]. وتُدمِج 'الاتصالات كخدمة' التي تقدمها منظمات الاتصالات بين قدرات الاتصالات والإنترنت. ويؤدي هذا التقارب إلى تفرد 'الاتصالات كخدمة' ببعض السمات المعرَّضة لمخاطر محددة. وتحدد هذه التوصية هذه المخاطر وتوصي بالمتطلبات الأمنية اللازمة للتصدي لها.

وتراعي هذه التدابير اللازمة الالتزامات القانونية والتنظيمية الوطنية في فرادى الدول الأعضاء المشغِّلة للاتصالات كخدمة. ويستند نص هذه التوصية إلى المنهجية المحددة في القسم 10 من التوصية [ITU-T X.1601].

2 المراجع

تضم التوصيات التالية وسائر المراجع الصادرة عن قطاع تقييس الاتصالات (ITU-T) أحكاماً تشكل، من خلال الإشارة إليها في هذا النص، أحكاماً تتعلق بهذه التوصية. وكانت الطبعات المشار إليها سارية المفعول في وقت النشر. وتخضع جميع التوصيات وغيرها من المراجع للتنقيح؛ ولذلك، يُشجع مستعملو هذه التوصية على تقصي إمكانية تطبيق أحدث طبعة من التوصيات وسائر المراجع المدرجة أدناه. وتنشر بانتظام قائمة بتوصيات قطاع تقييس الاتصالات (ITU-T) السارية المفعول. ولا تعني الإشارة إلى وثيقة معينة داخل هذه التوصية اكتساب تلك الوثيقة، في حد ذاتها، صفة التوصية.

[ITU-T X.1601] التوصية ITU-T X.1601 (2015)، *إطار أمني للحوسبة السحابية*.

[ITU-T X.1602] التوصية ITU-T X.1602 (2016)، *متطلّبات الأمن من أجل بيئات تطبيقات البرمجية كخدمة*.

[ITU-T Y.3501] التوصية ITU-T Y.3501 (2016)، *الحوسبة السحابية – الإطار والمتطلبات رفيعة المستوى*.

3 التعاريف

1.3 مصطلحات معرّفة في وثائق أخرى

تعرِّف هذه التوصية المصطلحات التالية المعرَّفة في وثائق أخرى:

1.1.3 استيقان [ITU-T X.1601]: التحقّق من هوية المستعمل أو العملية أو الجهاز، غالباً كشرط أساسي للسماح بالنفاذ إلى الموارد في نظام المعلومات.

2.1.3 قدرة [b-ISO 15531-1]: القدرة على أداء نشاط معين.

3.1.3 الحوسبة السحابية [b-ITU-T Y.3500]: نموذج للتمكين من النفاذ الشبكي إلى مجموعة قابلة للزيادة ومرنة من الموارد المادية أو الافتراضية التي يمكن تقاسمها والتزود بها وإدارتها على أساس الخدمة الذاتية وعند الحاجة.

ملاحظة – تشمل أمثلة الموارد المخدمات وأنظمة التشغيل والشبكات والبرمجيات والتطبيقات ومعدات التخزين.

4.1.3 خدمة سحابية [b-ITU-T Y.3500]: قدرة أو عدد أكبر من القدرات تُقدم عن طريق الحوسبة السحابية وتُلبى باستخدام سطح بيني معلن.

5.1.3 عميل الخدمة السحابية [b-ITU-T Y.3500]: طرف يكون مرتبطاً بعلاقة تجارية لأغراض استخدام الخدمات السحابية.

ملاحظة – لا تستوجب العلاقة التجارية بالضرورة وجود اتفاقات مالية.

6.1.3 شريك في الخدمة السحابية [b-ITU-T Y.3500]: طرف يشارك في دعم أنشطة مقدم الخدمة السحابية أو عميل الخدمة السحابية أو كليهما، أو يساعد في القيام بها.

7.1.3 مقدم الخدمة السحابية [b-ITU-T Y.3500]: طرف يتيح توافر الخدمات السحابية.

8.1.3 مستعمل الخدمة السحابية [b-ITU-T Y.3500]: شخص طبيعي أو كيان يعمل بالنيابة عنه يرتبط بأحد عملاء الخدمة السحابية ويستعمل الخدمات السحابية.

ملاحظة – تشمل أمثلة هذه الكيانات الأجهزة والتطبيقات.

9.1.3 الاتصالات كخدمة (CaaS) [b-ITU-T Y.3500]: فئة من الخدمات السحابية تكون فيها القدرة المقدّمة لعميل الخدمة السحابية متمثلة في التفاعل والتعاون في الوقت الفعلي.

ملاحظة – يمكن للاتصالات كخدمة أن توفر قدرات من نوع قدرات التطبيق ومن نوع قدرات المنصة على السواء.

10.1.3 تعدد الشاغلين [b-ITU-T Y.3500]: توزيع الموارد المادية والافتراضية بحيث يتم عزل الشاغلين المتعددين وحساباتهم وبياناتهم عن بعضهم البعض، ويكون النفاذ غير ممكن فيما بين بعضهم البعض.

11.1.3 التنسيق [b-ITU-T Y.3100]: في سياق الاتصالات المتنقلة الدولية–2020 (IMT-2020)، العمليات الهادفة إلى الترتيب التلقائي للوظائف والموارد الشبكية في البنى التحتية المادية والافتراضية، على السواء، وتنسيقها وإنشاء أمثلة لها واستخدامها، تلقائياً، باستخدام معايير تحقق المستوى الأمثل من هذه العمليات.

12.1.3 البرمجيات كخدمة (SaaS) [b-ITU-T Y.3500]: فئة من الخدمات السحابية تكون فيها القدرات السحابية المقدمة لعميل الخدمة السحابية من نوع قدرات التطبيقات.

2.3 المصطلحات المعرفة في هذه التوصية

لا توجد.

4 الاختصارات والأسماء المختصرة

تُستخدم في هذه التوصية الاختصارات والأسماء المختصرة التالية:

CaaS الاتصالات كخدمة *(Communications as a Service)*

CSC عميل الخدمة السحابية *(Cloud Service Customer)*

CSN شريك في الخدمة السحابية *(Cloud Service Partner)*

CSP مقدِّم الخدمة السحابية *(Cloud Service Provider)*

CSU مستعمِل الخدمة السحابية *(Cloud Service User)*

DDoS الحرمان من الخدمة الموزَّع *(Distributed Denial of Service)*

GSM النظام العالمي للاتصالات المتنقلة *(Global System for Mobile)*

IAM إدارة خدمات الهوية والنفاذ *(Identity and Access Management)*

IaaS البنية التحتية كخدمة *(Infrastructure as a Service)*

ID معرِّف هوية *(Identifier)*

MMS خدمة الرسائل متعددة الوسائط *(Multimedia Messaging Service)*

NaaS الشبكات كخدمة *(Network as a Service)*

OS نظام التشغيل *(Operating System)*

PaaS المنصات كخدمة *(Platform as a Service)*

PC الحاسوب الشخصي *(Personal Computer)*

QR الاستجابة السريعة *(Quick Response)*

SaaS البرمجيات كخدمة *(Software as a Service)*

SDK مجموعة أدوات تطوير البرمجيات *(Software Development Kit)*

SIM وحدة هوية المشترك *(Subscriber Identity Module)*

SMS خدمة الرسائل القصيرة *(Short Message Service)*

URL محدِّد مواقع الموارد الموحَّد *(Uniform Resource Locator)*

(U)SIM وحدة تعرّف هوية المشترك (العالمية) *((Universal) Subscriber Identity Module)*

VoLTE نقل الصوت بتكنولوجيا التطور الطويل الأجل *(Voice over Long-Term Evolution)*

VPN شبكة خاصة افتراضية *(Virtual Private Network)*

5 الاصطلاحات

لا فرق في هذه التوصية بين 'المخدِّم' و'المخدِّم الافتراضي'.

6 نظرة عامة على الاتصالات كخدمة

يرد تعريف خدمة 'الاتصالات كخدمة' (CaaS) في القسم 9.1.3 من هذه التوصية. وقد أوصِي بأن يكون الانفتاح في قدرات الاتصالات، ودعم برمجيات الاتصالات، والاتصالات الموحّدة المتطلبات العامة لخدمة CaaS (انظر القسم 11 من التوصية [ITU-T Y.3501]).

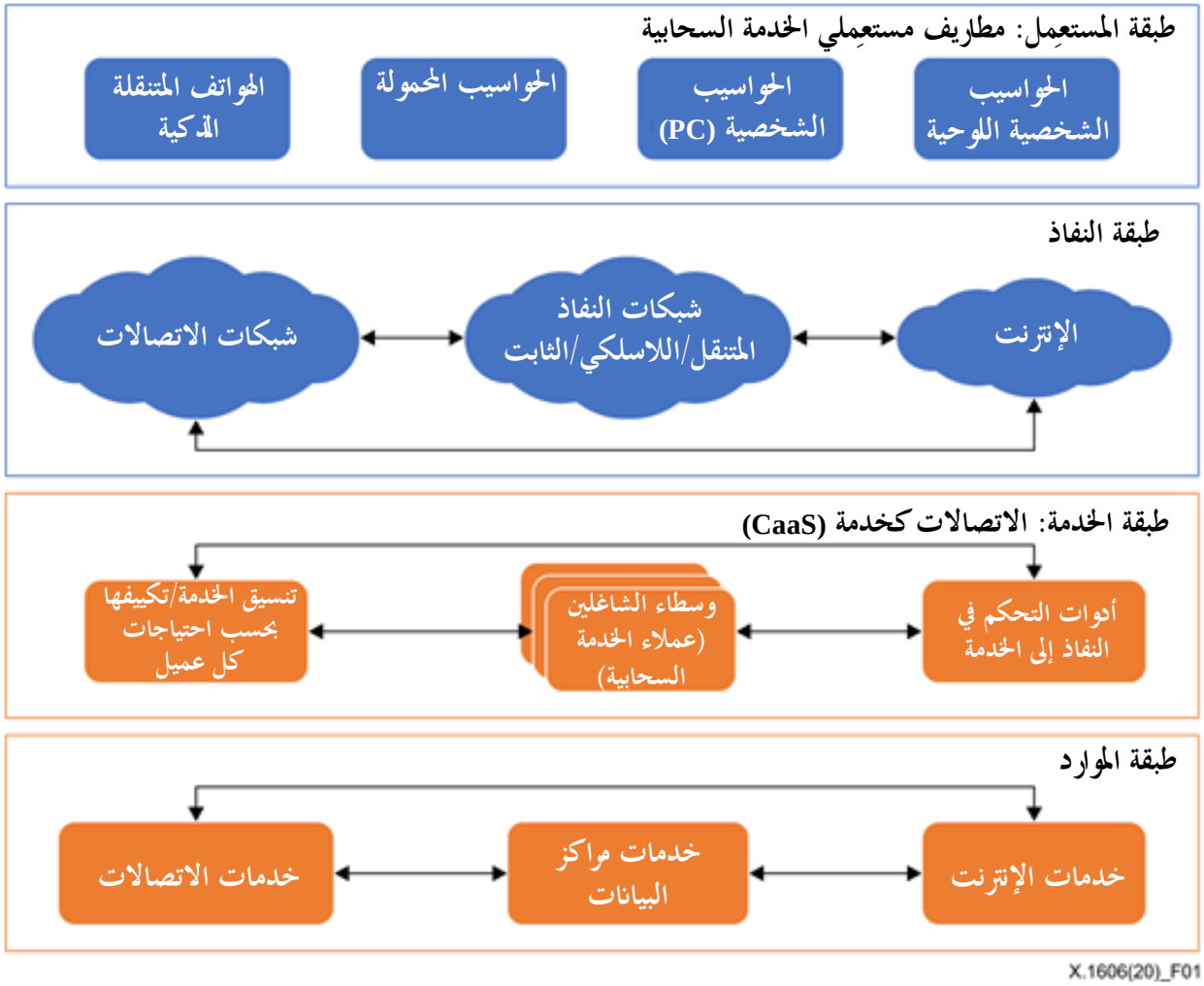
ووفقاً للممارسة المعتمدة في دوائر الصناعة، عادةً ما تُنفِّذ 'الاتصالات كخدمة' القدرات التالية أو تدعمها:

- مزيج من خدمات الاتصالات وخدمات الإنترنت؛
- الاتصال في الزمن الفعلي؛
- التزامن بين عدة أجهزة؛
- عزل موارد الاتصالات؛
- تحديث بيانات وجود المستعمِل؛
- الدردشة أو الاجتماعات الجماعية؛
- الدمج في برمجيات أخرى من 'البرمجيات كخدمات'؛
- الاشتراك في الخدمة أو تركها؛
- تكييف عمليات الخدمات بحسب احتياجات كل عميل؛
- تقاسم البيانات أو الملفات؛
- إدارة الهوية والنفاذ (IAM).

ويصف الشكل 6-1 نموذجاً عاماً لخدمة CaaS، حيث توجد أربع طبقات موسومة كالتالي: المستعمِل؛ النفاذ؛ الخدمة؛ الموارد.

- طبقة المستعمِل: تحتوي على مطاريف مستعمِلي الخدمة السحابية (CSU) القادرة على إدارة بعض عملاء خدمة CaaS والنفاذ إلى الإنترنت بل حتى شبكات الاتصالات.
- طبقة النفاذ: توفر أنماطاً متنوعة من الأنفاق للسماح عادةً بنفاذ المطاريف إلى خدمة CaaS التي تستهدفها.

- طبقة الخدمة: وهي أيضاً طبقة CaaS، يمتلكها مقدِّم للخدمة السحابية (CSP) يعتمد على الموارد الداخلية والخارجية اللازمة لإتمام عمل الخدمة. وتؤدي طبقة الخدمة مهام تكييف عمليات الخدمة بحسب احتياجات كل من عملاء الخدمة السحابية (CSC) وتوزيع الموارد لهم، والاحتفاظ بشبكة خدمة دينامية (افتراضياً) لعميل الخدمة السحابية مع مستعملي الخدمة السحابية (CSU) المنتسبين إلى هذا العميل، وعزل موارد الحوسبة وشبكات الاتصالات الخاصة بأي من عملاء الخدمة السحابية.
- طبقة الموارد: توفر موارد البنية التحتية الأساسية، المتعلقة بمعالجة البيانات واتصالاتها، وقد يكون جزء منها بنى تحتية كخدمة (Iaas) ومنصات كخدمة (PaaS) وشبكات كخدمة (NaaS).



الشكل 1 – نموذج عام لخدمة 'الاتصالات كخدمة' (CaaS)

وفي القسمين المتبقيين من هذه التوصية:

- يحلل القسم 7 التهديدات الأمنية التي قد تتعرض لها 'الاتصالات كخدمة' (CaaS) وتستهدف طبقة أو أكثر من الطبقات الأربع.
- ويوصي القسم 8 بالمتطلبات الأمنية اللازمة 'للاتصالات كخدمة' من أجل التصدي للتهديدات التي تستهدف ثلاث طبقات هي:
  - طبقة مطاريف مستعملي الخدمة السحابية؛
  - طبقة الاتصالات كخدمة؛
  - طبقة موارد الخدمة.

ولا تشمل هذه التوصية طبقة النفاذ، ذلك أن خدمة CaaS لا تتحكم في القدرات الأمنية لهذه الطبقة، مع أنه يمكن لهذه الخدمة ومستعملي الخدمة السحابية تقييم مستوى أمن طبقة النفاذ أو مراقبته.

7 التهديدات الأمنية التي قد تتعرض لها الاتصالات كخدمة

إن التهديدات والتحديات الأمنية التي قد تتعرض لها الحوسبة السحابية، المحددة في التوصية [ITU-T X.1601] (والمسرودة أيضاً في التذييل I لهذه التوصية)، قد تنطبق على عدة سيناريوهات لخدمة 'الاتصالات كخدمة' (CaaS). فضلاً عن ذلك، تُحدد في الفقرات من 1.7 إلى 8.7 من هذه التوصية بعض التهديدات المحددة التي قد تتعرض لها خدمة CaaS.

1.7 التهديدات التي تستهدف الهوية

تشكل قدرات الاتصالات الموحّدة نواةَ الاتصالات كخدمة (CaaS)، وهي تختلف اختلافاً طفيفاً عن قدرات 'البرمجيات كخدمة' (SaaS). إذ تُدمج خدمة CaaS قدرات الاتصالات فيما بين المطاريف وتعززها بالاستخدام الفعّال للحوسبة السحابية. وتدعم أي خدمة CaaS معظم الأنماط السائدة للمطاريف أو أنظمة التشغيل (OS) كالهواتف الذكية أو الحواسيب الشخصية (PC).

وبالتالي، فقد تتعرض خدمة CaaS في نموذج الاتصالات من عدة نقاط إلى عدة نقاط لبعض التهديدات الخاصة في حال تعرّض الهوية لانتهاك.

1.1.7 سرقة إثباتات الهوية

لراحة مستعملي الخدمة السحابية (CSU)، تعتمد العديد من خدمات 'الاتصالات كخدمات' (CaaSs) حلاً استيقانياً يدعم الاستيقان من الأرقام المتنقلة (أي معرفات الهوية (ID) للاتصالات المتنقلة) أو الاستيقان من اسم المستعمِل وكلمة السر، أو من كليهما. وفي هذه الحالة، يمكن تشكيل اسم المستعمِل المحدد آلياً في الحل بحيث يكون كمعرِّف هوية الهاتف المتنقل. علاوةً على ذلك، تدعم بعض خدمات CaaS منح مستعمِل الخدمة السحابية الواحد معرِّفاً واحداً للهوية يتيح له النفاذ إلى الخدمة بعدة مطاريف في آن واحد، أو تدعم تزامن التسلسل التاريخي للاتصالات فيما بين عدة مطاريف.

ويعتمد أمن الاستيقان من الأرقام المتنقلة اعتماداً كبيراً على الثقة في كل من الاستيقان، والتجفير الذي يُجريه مشغِّل الشبكة المتنقلة، وبطاقة وحدة تعرّف هوية المشترِك (العالمية) (U) SIM)) المحتوية على الإثبات (الإثباتات). إذ توجد في الشبكات المتنقلة، وخاصة في شبكات تحالف النظام العالمي للاتصالات المتنقلة (GSMA)، بعض مواطن الضعف (المثبتة عملياً) التي قد تُزعزع الثقة فيها وتؤدي إلى سرقة إثباتات الهوية (مؤقتاً). فيمكن، مثلاً، أن تُستنسخ مادياً بعض بطاقات وحدة تعرّف هوية المشترِك (SIM)؛ أو تُعترَض بعض شفرات الاستيقان الدينامية المنقولة بخدمة الرسائل القصيرة (SMS) في شبكات اتصالات النظام العالمي للاتصالات المتنقلة (GSM). كما يمكن أن يُساء استخدام مفاتيح التجفير المؤقتة المعترَضة في اختطاف معرِّف الهوية مؤقتاً في صمت.

فضلاً عن ذلك، قد تمنح عملية الاستيقان من اسم المستعمِل وكلمة السر مُنتهِكَ الهوية الفرصة لاستخدام هذا النمط من أنماط الاستيقان مع مطاريف أخرى محدَّدة لمراقبة مستعمِل الخدمة السحابية (بالتزامن). فعلى سبيل المثال، إذا استطاع المنتهِك التعامل مع مطرافٍ متنقلٍ لأحد مستعملي الخدمة السحابية مزوَّدٍ ببطاقة SIM (U) أو بإثباتات بطاقة SIM افتراضية، يمكنه الحصول على اسم المستعمِل الموجود في الذاكرة المخفية واستخدام آلية إعادة التحديد لتحديد كلمة سر جديدة والاحتفاظ بها في الذاكرة المخفية بالمطراف. وبالتالي، فمن الممكن ألا يدرك مستعمِل الخدمة السحابية أنه قد أُعيد تحديد كلمة السر، وأن يراقب المنتهِك، بصمت، محتوى اتصالات المستعمِل الجارية بل حتى تسلسلها التاريخي.

2.1.7 تزييف الهوية

بمجرد سرقة المنتهِك لإثباتات هوية مستعمِل الخدمة السحابية أو حصوله عليها، يمكنه إساءة استخدامها في النفاذ إلى الخدمة التي يقدمها عميل خدمة سحابية ينتسب إليه مستعمِل الخدمة السحابية ذاك. وفي الوقت ذاته، يستطيع منتهِك الهوية أيضاً الحصول على أي كيان اجتماعي له نفس إثبات هوية مستعمِل الخدمة السحابية، أو حتى تزييف كيان اجتماعي آخر، أو إنشاء كيان جديد، وهو ما يمكن أن تبيّنه أولاً وظيفة وجود المستعمِل.

فوجود المستعمِل سمةٌ عامة في خدمة CaaS، تُنفَّذ عادةً بإعداد صورة ذاتية لمستعمِل الخدمة السحابية مؤلفة من صورة شخصية صغيرة الحجم ونص محدود. وعن طريق بيانات وجود المستعمِل هذه، يمكن لمستعمِلي الخدمة السحابية المنتسبين إلى عميل الخدمة السحابية ذاته الحصول على اعتراف سريع بهوياتهم من أي مستعمِلٍ منهم. إلا أن بيانات وجود المستعمِل المتصلة بهوية منتهَكة قد تزوَّر ويُساء استخدامها في أنشطة احتيالية. فعلى سبيل المثال، يستطيع منتهِك الهوية الاستيلاء على بيانات مالية سرية لإحدى الشركات من أحد محاسبيها بتزوير بيانات وجود المستعمِل المنتهكَة هويته على أنه عضو في مجلس إدارة الشركة.

ونظراً إلى أن التصوير الفيديوي في الوقت الفعلي هو أحد التشكيلات القياسية للاتصالات كخدمة، فيمكن أيضاً تزوير المشهد الذي تبيّنه الهوية المنتهَكة عبر البث الفيديوي بغرض تعزيز أصالة الكيان الاجتماعي والنشاط الاحتيالي.

2.7 التهديدات المتصلة بإدارة دورة حياة الحسابات

قد يكون لأي مستعمِل للخدمة السحابية أو عميلها أو مقدِّمها الحق في إلغاء أي حساب يخضع لسلطته. وفي دورة الحياة العامة للحسابات، حينما يتقرر إلغاء أي حساب، ينبغي الاتفاق مسبقاً على التصرّف المفترَض من طرف مقدِّم الخدمة السحابية فيما يتعلق بنقل محتوى الحساب والمعلومات المتعلقة به عن طريق خدمة 'الاتصالات كخدمة' (CaaS) كلها، أي على مدى إمكانية احتفاظ عميل الخدمة السحابية بهذه البيانات في فضائه المنطقي أو مدى إمكانية احتفاظ مستعمِل الخدمة السحابية بها في مِطرافه.

والتخلص من المطراف أو سرقته قد يعني أيضاً ضرورة حذف أي معلومات متعلقة بالحساب من الذاكرة المخفيّة، وأي بيانات متصلة بها.

3.7 التهديد المتصل بعملية التنسيق

بوظيفة التنسيق (انظر التوصية [b-ITU-T Y.3100])، يمكن لعميل الخدمة السحابية تكييف عملياته وقدراته المتعلقة بالخدمة بحسب احتياجاته ذاتياً أو عن طريق مقدِّم الخدمة السحابية الخاص به. فيستطيع عميل الخدمة السحابية، مثلاً، تكييف عملية وامتياز إدارة العضوية في مجموعة دردشة، وكذلك خفض أو زيادة درجة تقييد مدى إمكانية بحث عميل الخدمة السحابية عن بيانات الاتصال.

وفيما يتعلق بمتطلبات العملاء، يستطيع مقدِّم الخدمة السحابية تمكين أكثر من عميلَيْن من عملاء الخدمة السحابية من تقاسم بيانات الاتصال الخاصة بكل منهم بل حتى الاتصال مباشرة ببعضهم بعضاً، كما يمكنه دمج أكثر من عميل من عملاء الخدمة السحابية في عميل أكبر حجماً.

علاوةً على ذلك، فلتنفيذ سمة خدمة جديدة، يمكن لمقدِّم الخدمة السحابية تخفيف أو تشديد الشروط الأمنية اللازمة على الشبكة التي يمكن لمستعمِل الخدمة السحابية النفاذ إليها.

وإجراء أي تنسيق دون إيلاء اعتبار تام لعنصر الأمن قد يؤثر سلباً على عملية عزل المعلومات عن الخدمات. فعلى سبيل المثال، إذا نُسقت خدمة CaaS التي يقدمها عميل الخدمة السحابية بحيث تُدمَج فيها الخدمة الصوتية وخدمة الرسائل الخاصة بإحدى شبكات النظام العالمي للاتصالات المتنقلة (GSM)، فمن المستحيل تقريباً تنفيذ سمة العزل من طرف إلى آخر نظراً إلى أن كيانات الشبكة GSM تعتمد تكنولوجيات قديمة ولا يمكنها دعم أي نوع من أنواع سمات العزل. وفي حال سماح إجراء التنسيق لنمط شبكة غير مأمون بدعم سمة خدمية أكثر مرونةً، فقد تزيد هذه الشبكة من مستوى تعرض الاتصالات كخدمة للخطر أكثر من بعض عملاء الخدمة السحابية. فمثلاً، إذا أُعيد تشكيل صفة متطلب النفاذ إلى الشبكة الخاصة الافتراضية (VPN) كأسلوب عزل من الإلزامي إلى الاختياري لضمان جودة الدردشة الفيديوية في الاتصالات كخدمة، قد يزداد خطر التنصّت.

4.7 التهديد المتصل بسياق المطاريف

قد يكون السياق الأمني للمطاريف في خدمة 'الاتصالات كخدمة' (CaaS) متقلّباً، خاصة إذا كانت المطاريف هواتف ذكية أو أجهزةً محمولة. وقد يكون هذا السياق أعقد إذا كانت هذه المطاريف ممتلكاتٍ شخصية، إذ قد يستخدمها أقارب مستعمِل الخدمة السحابية أو ضيوفه. وتجدر الإشارة إلى أنه يمكن عرض شاشة المطراف على شاشة أخرى أو وَصْلها بها بحيث يمكن تسجيل وجود شاشة

غير معروفة. وفي شبكة غير مُؤمَّنة، يمكن لمواطن ضعف المطراف أن تكون مكشوفةً لأي مُهاجم على نحو أكثر مباشرةً. كما أنه يمكن فك تجفير محتوى الاتصالات عبر خدمة CaaS وتخزينه في مطراف. وقد تؤدي كل هذه الحالات إلى تسرّب البيانات.

وفي حال تمكّن المهاجم من التحكم في المطراف (عن بُعد أو محلياً)، يمكنه إساءة استخدامه في استغلال مواطن ضعف خدمة CaaS بل حتى مستعمِل الخدمة السحابية بها. وفي حال التحكم في عدة مطاريف في آن واحد من خلال برمجية روبوتية، قد يشنّ المهاجم أيضاً هجمةً من نمط الحرمان من الخدمة الموزَّع (DDoS).

5.7 التهديد المتمثل في الرسائل الاقتحامية، وتوزيع البرمجيات الضارة

من الممكن التحرّش بمستعمِل الخدمة السحابية أو حتى تَصيُّده عن طريق هجمة رسائل اقتحامية يوجهها إليه مستعملون آخرون للخدمة السحابية عبر خدمة 'الاتصالات كخدمة' (CaaS). ففي معظم الحالات يصعب بالفعل على مستعمِل الخدمة السحابية أن يحدد منطقياً ما إذا كان يمكنه الوثوق في المعلومات الواردة في محدّدِ مواقع قصير من محدِّدات مواقع الموارد الموحَّدة (URL) أو في إحدى شفرات الاستجابة السريعة (QR)، مما قد يُودي به إلى النفاذ إلى موقع إلكتروني احتيالي أو تنزيل برمجيات ضارة.

6.7 التهديد المتصل بالخدمات الإضافية

من الطبيعي أن تقدم خدمة CaaS بعض الخدمات الإضافية بناءً على الخدمة الأساسية فيها، كتقاسم الملفات، ومتصفِّح الويب المدمج، ونظام إدارة المحتوى، بل حتى الأعمال التجارية الإلكترونية. وفي معظم الحالات، تكون هذه الخدمات الإضافية بسيطة إلى حد ما.

غير أن مواطن ضعف هذه الخدمات الإضافية قد تُعرِّض الاتصالات كخدمة نفسها لتهديدات كبيرة. فعلى سبيل المثال، قد يؤدي النَّقْر على موقع URL قصير غير مأمون إلى استدعاء تمديدات متصفِّح الويب غير القادرة على التصدي لعنوان ويب خطير، وبالتالي يزداد إلى حد كبير احتمال الإخلال بأمن مستعمِل الخدمة السحابية بل حتى أمن خدمة CaaS.

وقد تُوجِّه بعض الخدمات الإضافية مستعمِل الخدمة السحابية إلى ترك خدمته الحالية للاتصالات كخدمة والانتقال إلى خدمة أخرى احتيالية. فإن لم يدرك المستعمِل هذا الانتقال، لن يستطيع تعديل مستوى ثقته على النحو اللازم وفي الوقت المناسب، الأمر الذي سيتسبب في وقوع أضرار واسعة النطاق (كاستغلال المزيد من مواطن الضعف، الابتزاز، استخدام برمجيات طلب الفدية، إلخ.).

7.7 التهديد المتصل بمجموعة أدوات تطوير البرمجيات

يمكن أن تقدم خدمة CaaS مجموعة أدوات لتطوير البرمجيات (SDK) لتشجيع التكامل مع تطبيقات أو برمجيات كخدمات أخرى. ويعني التكامل الثقة أساساً إلى حد ما بين خدمة CaaS ومستعمِل مجموعة أدوات SDK فيها. وبالتالي، فقد تزيد مواطن الضعف الخاصة بمستعمل مجموعة أدوات SDK من تهديدات تعرض الاتصالات كخدمة للهجمات أو سوء الاستخدام.

ونظراً إلى إمكانية احتواء المطراف على عدة إثباتات لهويات عملاء مختلفين للخدمة السحابية، يمكن لمستعمِل مجموعة أدوات SDK في خدمة CaaS إساءة استخدام هذه الإثباتات في النفاذ على نحو غير قانوني إلى عملاء آخرين للخدمة السحابية.

8.7 التهديدات الناشئة عن مواطن ضعف شبكات الاتصالات

في حال اشتمال خدمة CaaS على قدرات أخرى بالإضافة إلى قدرة النفاذ إلى الإنترنت يزوّدها بها مشغِّل شبكة الاتصالات، من قبيل خدمة الرسائل القصيرة (SMS) وخدمة نقل الصوت بتكنولوجيا التطور الطويل الأجل (VoLTE) والنداءات الجماعية عبر دارة اتصال وخدمة الرسائل متعددة الوسائط (MMS) والخدمات القائمة على الموقع، قد يؤثر مستوى أمن شبكة الاتصالات تأثيراً مباشراً على الاتصالات كخدمة.

فنجاح أي إساءة استخدام لمواطن ضعف شبكة الاتصالات قد يؤدي إلى تسرّب البيانات من الاتصالات كخدمة. وبالمثل، قد يؤدي نجاح أي هجمة على شبكة الاتصالات، وخاصة على العُقد الموصولة بمخدِّمات الاتصالات كخدمة، إلى توسيع رقعة السطح المعرَّض للتهديد في هذه الخدمة.

فضلاً عن ذلك، فنظراً إلى قدرة المطاريف الحديثة المتاحة تجارياً على التبديل بين شبكات النفاذ والشبكات الخاصة الافتراضية تبديلاً نشطاً فيما بين مورّدي هذه الشبكات، وفقاً لسياسات محددة سلفاً، وعدم إيلائها اعتباراً كافياً لمدى الثقة في شبكة النفاذ ومدى أصالتها، قد لا يدرك مستعمِل الخدمة السحابية استخدامه لبيئة شبكية غير مأمونة، الأمر الذي قد يؤدي إلى تسرّب معلومات سرية.

8 المتطلبات الأمنية للاتصالات كخدمة

تنطبق المتطلبات الأمنية اللازمة للبرمجيات كخدمة المحددة في التوصية [ITU-T X.1602] على سيناريوهات الاتصالات كخدمة. فضلاً عن ذلك، يحدد هذا القسم بعض المتطلبات الأمنية الإضافية اللازمة للتصدي للتهديدات المحددة في القسم 7 من هذه التوصية.

1.8 إدارة الهوية والنفاذ

1.1.8 إدارة الهوية

ينبغي أن تعيّن خدمة 'الاتصالات كخدمة' (CaaS) حداً أقصى من المطاريف العاملة بالتزامن التي تشترك في امتلاك إثباتات الهوية ذاتها. ويمكن للخدمة CaaS التحقق من تزويد مطراف معين بالوسائل اللازمة لتعرّف هوية العتاد والخدمات ليكون المتحكِّم الرئيسي الذي يمكنه أن يأذن لسائر المطاريف بالنفاذ بناءً على طلبها.

وبإمكان خدمة CaaS رصد المطاريف العاملة بالتزامن بنفس إثبات الهوية والاستمرار في إبلاغ جميع المطاريف (أو المطراف المتحكِّم الرئيسي، على الأقل) بالحالة الراهنة للمطاريف الأخرى العاملة بالتزامن. ويستطيع مستعمِل الخدمة السحابية استخدام المطراف المتحكِّم الرئيسي، أو وسيلة استيقان أكثر مأمونيةً (كالاستيقان من حدوث تجاوز من عدمه)، لإجبار مطراف محدد على الخروج من دورة الاتصال ومنع أي محاولات مستقبلية لنفاذه إلى الخدمة، بل حتى لحذف المعلومات المتبقية فيه.

ويمكن أن تأخذ خدمة CaaS في اعتبارها توجيه مستعمِل الخدمة السحابية إلى استخدام إثباتات هوية مختلفة (وكلمات سر مختلفة، على الأقل) لعملاء الخدمة السحابية المختلفين، وهو ما يمكن أن يحدّ من خطر استخدام إثبات هوية مسروق في النفاذ إلى عدة عملاء للخدمة السحابية.

2.1.8 التحكم في النفاذ

لما كان عمل المطاريف بالتزامن بإثبات هوية واحد من القدرات العامة لخدمة CaaS، فمن المفيد السماح لهذه الخدمة بالحصول على بيانات الموقع الجغرافي للمطاريف وتحديثها بما يمكّنها من اكتشاف أي مظاهر شاذة في حالة النفاذ إلى المطاريف. ونظراً إلى إمكانية نفاذ مطراف واحد إلى عدة شبكات في آن واحد، يمكن أن تولي خدمة CaaS اعتباراً لإمكانية استخدام معلومات متعددة الأبعاد للتحقق من صحة الموقع بمقارنته بها.

وفي حال عدم إمكانية ضمان أمن الشبكة، قد يكون استخدام شبكة خاصة افتراضية (VPN) خياراً جيداً لتعزيز أمن البنية التحتية. فينبغي أن تأخذ خدمة CaaS في اعتبارها إلزام مستعمِل الخدمة السحابية أو عميلها باستعمال خدمة إلزامية في شبكة خاصة افتراضية، ومنع مستعمِل الخدمة السحابية أو عميلها من اعتماد أي خدمات أخرى في الشبكة الخاصة الافتراضية كقفزة أو ترحيل من أجل النفاذ إلى الخدمة الإلزامية في تلك الشبكة. وقد يؤدي استخدام شبكة خاصة افتراضية اختيارية أو غير موثوق بها إلى حجب موقع المطراف ويزيد أيضاً من خطر تعرضه لهجمات من وُسطاء.

علاوةً على ذلك، ففي حال عدم قبول عميل الخدمة السحابية خطر استقبال رسالة SMS معتَرَضة لإحدى شبكات GSM، ينبغي أن تأخذ خدمة CaaS في اعتبارها رصد أنماط الشبكات التي يَنفُذ إليها جميع مستعملي الخدمة السحابية، ثم رفض استخدام رسالة SMS كأسلوب استيقان إذا كان مستعمِل الخدمة السحابية مغطّىً بإحدى شبكات GSM. وكبديلٍ آخر، يمكن أن تستبعد خدمة CaaS ببساطة مورد رسالة SMS لشبكة GSM من أجل عميل الخدمة السحابية.

3.1.8 التحقق من الهوية

بالنظر إلى قدرة مستعمِل الخدمة السحابية على استخدام معلومات غير واضحة أو غير دقيقة أو حتى مزيفة لإنتاج صورة ذاتية له، ينبغي أن تنبّه خدمة CaaS جميع مستعملي الخدمة السحابية من تحقق طرف ثالث موثوق به من إحدى الهويات

الاجتماعية الموجودة في جهات الاتصال الخاصة بهم. وقد يكون الطرف الثالث عميلاً للخدمة السحابية، أو خدمةَ CaaS نفسها، أو أي هيئة أخرى مستقلة. ويمكن أن يكون إجراء التحقق إلزامياً أو اختيارياً، وإذا كان اختيارياً، فقد يلزم تنبيه مستعمِل الخدمة السحابية إلى عدم مسؤولية مقدِّم الخدمة السحابية أو عميلها عن مدى أصالة الهويات الاجتماعية الموجودة في عميل الخدمة السحابية.

وبما أن الهوية الاجتماعية أو التجارية لعميل الخدمة السحابية، التي يستخدمها ليصبح عميلاً لخدمة CaaS، قد تختلف تماماً عن هويته المعلنة، يُقترح أن تأخذ خدمة CaaS في اعتبارها مقارنة الهوية المعلنة التي يدّعيها عميل الخدمة السحابية بالمعلومات المتاحة لديها لدرء احتمال وقوع أي احتيال عام أو تجاري. فعلى سبيل المثال، قد يدّعي عميلٌ خبيث للخدمة السحابية أنه منظمة خيرية ويفرض على مستعمِل الخدمة بعض بنود التبرعات من أجل استغلاله.

4.1.8 إدارة الحسابات

نظراً إلى أنه يمكن لمستعمِل الخدمة السحابية امتلاك حساب واحد على الأقل في عميل واحد للخدمة السحابية، ويمكن لعميل الخدمة السحابية امتلاك حساب واحد على الأقل في خدمة CaaS، ينبغي أن تمنح خدمة CaaS مستعمِل الخدمة السحابية أو عميلها، وفقاً لمن تؤول إليه ملكية البيانات، امتيازَ النفاذ الكامل إلى بيانات الحساب. علاوةً على ذلك، ففي حال ضرورة إلغاء حساب أو حذفه، ينبغي أن توفر خدمة CaaS قدرةً موثوقة لتدمير بيانات الحساب مادياً في كل من المطراف والخدمة والشبكة، وفقاً لبنود التصريح القانوني لمالك البيانات.

2.8 أمن المطاريف

1.2.8 الأمن الداخلي

ينبغي أن توفر خدمة CaaS تدابير تقنية، كأداة أمنية أو وحدة أمنية مُدمجة في مطاريف مستعمِل الخدمة السحابية، لإجراء فحص أمني دوري أو بناءً على الطلب. ويمكن أن يقيّم هذا الفحص الأمني مدى وفاء سياق مطراف مستعمِل الخدمة السحابية بالمتطلبات الأمنية الإلزامية قبل نفاذه إلى خدمة CaaS. وإن لم يَجتَز مطراف المستعمِل الفحص الأمني، فمن الممكن أن تأخذ خدمة CaaS في اعتبارها رفض تقديم الخدمات (جزئياً). وفي الوقت ذاته، ينبغي أن توجّه خدمة CaaS مستعمِل الخدمة السحابية إلى تدارك المخاطر الأمنية المكتشَفة، أو يمكنها أن تُصلح هي مباشرةً مواطن الضعف هذه بإذنٍ من مستعمل الخدمة السحابية.

2.2.8 الأمن الخارجي

ينبغي أن توفر خدمة CaaS البرمجيات المستخدمة في مطاريف مستعمِل الخدمة السحابية. وينبغي أن توفر خدمة CaaS أيضاً منصة توزيع أو مصادر مأمونة للبرمجيات، تكون رسمية أو مرخصة. كما ينبغي أن تُعلن CaaS عن آلية التحقق اللازمة كي تستخدمها مطاريف المستعمِل للتحقق من أصالتها وسلامتها قبل تحديثها. وينبغي أن يكون نظام التشغيل أو البرمجية ذاتها الموجودان في مطاريف المستعمِل مزوّدين بقدرة الإعادة إلى الوضع السابق في حال إخفاق أي من عمليات التحديث.

وفي معظم الحالات، يكون التحديث الأمني لبرمجيات المطاريف إجراءً اختيارياً. إلا أنه في حال احتمال تَسبب أي موطن ضعف في المطراف في إلحاق ضرر بالغ بخدمة CaaS أو بأحد عملاء الخدمة السحابية أو حتى بمستعمِل آخر للخدمة السحابية، وفي حال إمكانية إصلاحه بإجراء تحديث أمني للمطراف، يمكن عندئذٍ أن تأخذ خدمة CaaS في اعتبارها رفض نفاذ مطراف مستعمِل الخدمة السحابية إلى الخدمة مؤقتاً قبل النجاح في تحديثه وفقاً للاتفاق المبرَم مع المستعمِل.

وفي معظم الحالات، توزّع خدمة CaaS برمجيات المطاريف توزيعاً عاماً. غير أنه في بعض الحالات قد يطلب عميل الخدمة السحابية برمجية مطراف مكيّفة بحسب احتياجاته هو ويطالب بمحدودية نطاق توزيعها، كأن توزَّع للعاملين التابعين له حصرياً. وفي هذه الحالة، ينبغي أن يكون توزيع البرمجية خاصاً. وقبل تنزيل البرمجيات أو تحديثها، يلزم الاستيقان منها في اتجاه ثنائي بين مستعمِل الخدمة السحابية وخدمة CaaS.

3.8 أمن الخدمات

1.3.8 أمن عملية التنسيق

قبل إجراء أو تشكيل أي تغيير في عملية التنسيق، من اللازم تقييم مدى تأثيره على الحدّ الأمني أو خفضه للمستوى الأمني أو مساسُه بعلاقة الثقة. وإذا كان يُحتمل أن تكون له بعض الآثار السلبية، ينبغي عندئذٍ إعادة التفاوض على المتطلبات أو الترتيبات الأمنية لخدمة 'الاتصالات كخدمة' (CaaS) الاتفاق عليها من جديد من طرف كل من مقدِّم الخدمة السحابية، وعميلها، وحتى مستعمِلها.

2.3.8 مكافحة الرسائل الاقتحامية

ينبغي أن تأخذ خدمة CaaS في اعتبارها دعم وظيفة لمكافحة الرسائل الاقتحامية كقدرة اختيارية لعميل الخدمة السحابية. كما ينبغي أن يأخذ مقدِّم الخدمة السحابية في اعتباره السماح لعميل الخدمة بأن يُدمج في خدمة CaaS الخاصة به وظيفة مكافحة للرسائل الاقتحامية يؤديها طرف ثالث. وتختلف القيود المفروضة على مدى إمكانية استخدام هذه الوظيفة وكيفية استخدامها باختلاف الاتفاقات المبرمة بين مقدمي الخدمة السحابية وعملائها ومستعمليها بشأن الخدمات واستعمالها.

فعلى سبيل المثال، إذا كان جميع مستعملي الخدمة السحابية موظفين تابعين لعميل الخدمة السحابية وكانت خدمة CaaS ذات الصلة تُستخدم لفائدة العميل حصرياً، يمكن حينئذٍ أن يكون الاتفاق المبرم بين مقدِّم الخدمة السحابية وعميلها كافياً للسماح باستخدام وظيفة لمكافحة الرسائل الاقتحامية.

وخلافاً لذلك، إذا كان بعض مستعملي الخدمة السحابية عملاء لعميل الخدمة، فيلزم في هذه الحالة أن يأذن هؤلاء المستعملون للعميل (ولمقدِم الخدمة السحابية) بمساعدتهم في مكافحة الرسائل الاقتحامية.

وبوجهٍ عام، ينبغي أن تتوفر وظيفة لمكافحة الرسائل الاقتحامية في المطراف أو السحابة أو في كليهما. وللاطلاع على التكنولوجيات البديلة المستخدمة لأداء هذه الوظيفة، انظر التوصيتين [b-ITU-T X.1244] و[b-ITU-T X.1246].

4.8 التنسيق الأمني

1.4.8 أمن الخدمات الإضافية ومجموعة أدوات تطوير البرمجيات

ينبغي أيضاً ألا تسمح خدمة CaaS إلا بالخدمات الإضافية التي اجتازت الفحص الأمني المتاح في الخدمة. وينبغي أن تساعد برمجيات المطاريف خدمة CaaS في رصد أي مظاهر شاذة في الخدمات الإضافية وتحليلها. ومن شأن استعانة خدمة CaaS بقائمة بيضاء أن يساعدها في الحد من قدرة الخدمة الإضافية على النفاذ إلى رابط خارجي أو اسم ميدان خارجي.

وفي حال لزوم نفاذ الخدمات الإضافية إلى بيانات العميل لتقديم الخدمة، يُشترط مسبقاً حصولها على إذنٍ واضح من مستعمِل الخدمة السحابية. ومن المفيد، في هذا السياق، إنشاء سجل واضح لحالات نفاذ الخدمات الإضافية إلى بيانات العملاء من أجل عمليات التدقيق فيما بعد.

وينبغي أن تكون مجموعة أدوات تطوير البرمجيات (SKD) في خدمة CaaS قادرةً على رصد وتحليل أي مظاهر شاذة في التطبيقات، أو 'البرمجيات كخدمة' المدمجة فيها هذه المجموعة. وينبغي أن تُجفِّر مجموعة أدوات SKD إثباتات الهوية وتعزلها تلافياً لاحتمال انتهاكها. فمثلاً، قد يضم التطبيق A والتطبيق B نفس مجموعة أدوات SKD وقد يتعايشان في المطراف ذاته لكن لا يمكن لأي منهما النفاذ إلى إثباتات هوية الآخر.

2.4.8 أمن البنى التحتية

ينبغي أن تعي خدمة CaaS التهديدات الناشئة عن البنى التحتية ذلك أنها تضم، على سبيل المثال، قدرات خدمات شبكات الاتصالات، كخدمة الرسائل القصيرة (SMS) وخدمة النداء الصوتي. وينبغي أن تأخذ خدمة CaaS في اعتبارها إنشاء بوابة بينها وبين شبكات الاتصالات بغرض رصد الرسائل الاقتحامية وانتهاكات الهوية المحتمل انتشارها من خدمات الاتصالات، أو مكافحتها، أو فرزها. ومن المفيد أن تنبّه خدمة CaaS مستعملي الخدمة السحابية إلى أنماط قنوات أو خدمات الاتصالات المستخدمة.

التذييل I

دليل سريع بشأن التهديدات والتحديات الأمنية المسرودة في التوصية ITU-T X.1601

(لا يشكل هذا التذييل جزءاً من هذه التوصية.)

كما ذُكر في القسم 7 من هذه التوصية، إن التهديدات والتحديات الأمنية التي قد تتعرض لها الحوسبة السحابية، المحددة في التوصية [ITU-T X.1601]، قد تنطبق على عدة سيناريوهات لخدمة 'الاتصالات كخدمة' (CaaS). ويسرد هذا التذييل جميع التهديدات والتحديات الأمنية المحددة في التوصية [ITU-T X.1601] غرض سرعة التحقق منها. وإن لزم الاطلاع على مزيد من التفاصيل، يُرجى الاطلاع على التوصية [ITU-T X.1601].

- التهديدات الأمنية للحوسبة السحابية
  - أ) التهديدات الأمنية لعملاء الخدمة السحابية (CSC)
    1) فقدان البيانات وتسربها
    2) النفاذ غير الآمن للخدمات
    3) التهديدات داخلية المصدر
  - ب) التهديدات الأمنية لمقدمي الخدمات السحابية (CSP)
    1) النفاذ غير المرخص إلى الإدارة
    2) التهديدات داخلية المصدر
- التحديات الأمنية للحوسبة السحابية
  - أ) التحديات الأمنية لعملاء الخدمة السحابية (CSC)
    1) غموض المسؤوليات
    2) فقدان الثقة
    3) غياب الإدارة
    4) فقدان السرية
    5) عدم تيسر الخدمة
    6) الحظر الذي يفرضه مقدم الخدمة السحابية
    7) سوء استعمال الملكية الفكرية
    8) فقدان سلامة البرمجيات
  - ب) التحديات الأمنية لمقدمي الخدمة السحابية (CSP)
    1) غموض المسؤوليات
    2) تقاسم البيئة
    3) عدم الاتساق والتضارب في آليات الحماية
    4) النزاع القضائي
    5) المخاطر التطورية
    6) سوء التحول والتكامل

7) عدم استمرارية الأعمال

8) الحظر الذي يفرضه الشريك في الخدمة السحابية

9) نقطة ضعف سلسلة التوريد

10) الاعتماد على البرمجيات

ج) التحديات الأمنية للشركاء في الخدمة السحابية (CSN)

1) غموض المسؤوليات

2) سوء استعمال الملكية الفكرية

3) فقدان سلامة البرمجيات.

التذييل II

التقابل بين التهديدات الأمنية والمتطلبات الأمنية

(لا يشكل هذا التذييل جزءاً من هذه التوصية.)

يربط هذا التذييل التهديدات المحددة في القسم 7 من هذه التوصية بالمتطلبات المحددة في القسم 8 منها.

الجدول I.1 التقابل بين التهديدات الأمنية والمتطلبات الأمنية المحددة في هذه التوصية

التهديدات المحددة في القسم 7 من التوصية		المتطلبات الموازية لها في القسم 8 من التوصية	
1.7	التهديدات التي تستهدف الهوية	1.8	إدارة الهوية والنفاذ
1.1.7	سرقة إثبات الهوية	1.1.8 2.1.8 4.1.8	إدارة الهوية التحكم في النفاذ إدارة الحسابات
2.1.7	تزييف الهوية	3.1.8 4.1.8	التحقق من الهوية إدارة الحسابات
2.7	التهديدات المتصلة بإدارة دورة حياة الحسابات	4.1.8	إدارة الحسابات
3.7	التهديد المتصل بعملية التنسيق	1.3.8	إدارة عملية التنسيق
4.7	التهديد المتصل بسياق المطاريف	2.8	أمن المطاريف
5.7	التهديد المتمثل في الرسائل الاقتحامية، وتوزيع البرمجيات الضارة	2.8 2.3.8	أمن المطاريف مكافحة الرسائل الاقتحامية
6.7	التهديد المتصل بالخدمات الإضافية	1.4.8	أمن الخدمات الإضافية ومجموعة أدوات تطوير البرمجيات
7.7	التهديد المتصل بمجموعة أدوات تطوير البرمجيات	1.4.8	أمن الخدمات الإضافية ومجموعة أدوات تطوير البرمجيات
8.7	التهديدات الناشئة عن مواطن ضعف شبكات الاتصالات	2.4.8	أمن البنى التحتية

بيبليوغرافيا

[b-ITU-T X.1244] Recommendation ITU-T X.1244 (2008), *Overall aspects of countering spam in IP-based multimedia applications*.

[b-ITU-T X.1246] Recommendation ITU-T X.1246 (2015), *Technologies involved in countering voice spam in telecommunication organizations*.

[b-ITU-T Y.3100] Recommendation ITU-T Y.3100 (2017), *Terms and definitions for IMT-2020 network*.

[b-ITU-T Y.3500] Recommendation ITU-T Y.3500 (2014) | ISO/IEC 17788:2014, *Information technology – Cloud computing – Overview and vocabulary*.

[b-ISO 15531-1] ISO 15531-1:2004, *Industrial automation systems and integration – Industrial manufacturing management data – Part 1: General overview*.

سلاسل التوصيات الصادرة عن قطاع تقييس الاتصالات

السلسلة A	تنظيم العمل في قطاع تقييس الاتصالات
السلسلة D	مبادئ التعريفة والمحاسبة والقضايا الاقتصادية والسياساتية المتصلة بالاتصالات/تكنولوجيا المعلومات والاتصالات على الصعيد الدولي
السلسلة E	التشغيل العام للشبكة والخدمة الهاتفية وتشغيل الخدمات والعوامل البشرية
السلسلة F	خدمات الاتصالات غير الهاتفية
السلسلة G	أنظمة الإرسال ووسائطه والأنظمة والشبكات الرقمية
السلسلة H	الأنظمة السمعية المرئية والأنظمة متعددة الوسائط
السلسلة I	الشبكة الرقمية متكاملة الخدمات
السلسلة J	الشبكات الكبلية وإرسال إشارات تلفزيونية وبرامج صوتية وإشارات أخرى متعددة الوسائط
السلسلة K	الحماية من التداخلات
السلسلة L	البيئة وتكنولوجيا المعلومات والاتصالات، وتغير المناخ، والمخلفات الإلكترونية، وكفاءة استخدام الطاقة، وإنشاء الكبلات وغيرها من عناصر المنشآت الخارجية وتركيبها وحمايتها
السلسلة M	إدارة الاتصالات بما في ذلك شبكة إدارة الاتصالات وصيانة الشبكات
السلسلة N	الصيانة: الدارات الدولية لإرسال البرامج الإذاعية الصوتية والتلفزيونية
السلسلة O	مواصفات تجهيزات القياس
السلسلة P	نوعية الإرسال الهاتفي والمنشآت الهاتفية وشبكات الخطوط المحلية
السلسلة Q	التبديل والتشوير، والقياسات والاختبارات المرتبطة بهما
السلسلة R	الإرسال البرقي
السلسلة S	التجهيزات المطرافية للخدمات البرقية
السلسلة T	المطاريف الخاصة بالخدمات التليماتية
السلسلة U	التبديل البرقي
السلسلة V	اتصالات البيانات على الشبكة الهاتفية
السلسلة X	**شبكات البيانات والاتصالات بين الأنظمة المفتوحة ومسائل الأمن**
السلسلة Y	البنية التحتية العالمية للمعلومات، والجوانب الخاصة ببروتوكول الإنترنت وشبكات الجيل التالي وإنترنت الأشياء والمدن الذكية
السلسلة Z	اللغات والجوانب العامة للبرمجيات في أنظمة الاتصالات

طُبعت في سويسرا
جنيف، 2021