الاتحـــــــــــاد الدولـــــــــــي للاتصـــــــــــالات

ITU-T

قطاع تقييس الاتصالات
في الاتحاد الدولي للاتصالات

X.1604

(2020/03)

السلسلة X: شبكات البيانات والاتصالات بين الأنظمة المفتوحة ومسائل الأمن

أمن الحوسبة السحابية – تصميم أمن الحوسبة السحابية

متطلبات أمن الشبكة كخدمة (NaaS) في الحوسبة السحابية

التوصية ITU-T X.1604

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
آمن 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 المنزلية	X.1119–X.1110
أمن الخدمات المتنقلة	X.1139–X.1120
أمن الويب	X.1149–X.1140
بروتوكولات الأمن	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
آمن 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)	
الاتصالات في حالات 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
آمن أنظمة النقل الذكية (ITS)	X.1389–X.1370
أمن تكنولوجيا سجل الحسابات الموزع	X.1429–X.1400
أمن تكنولوجيا سجل الحسابات الموزع	X.1449–X.1430
بروتوكولات الأمن (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
آمن 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
أشكال أخرى لأمن الحوسبة السحابية	X.1699–X.1680
الاتصالات الكمومية	X.1729–X.1700

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

التوصية ITU-T X.1604

متطلبات أمن الشبكة كخدمة (NaaS) في الحوسبة السحابية

ملخص

تحلل التوصية ITU-T X.1604 التهديدات والتحديات الأمنية التي تواجهها الشبكة كخدمة (NaaS) في الحوسبة السحابية وتحدد متطلبات الأمن للشبكة كخدمة في تطبيقات الشبكة كخدمة وجوانب منصات الشبكة كخدمة وتوصيلية الشبكة كخدمة استناداً إلى أنواع القدرات السحابية المقابلة.

التسلسل التاريخي

الطبعة	التوصية	تاريخ الموافقة	لجنة الدراسات	معرف الهوية الفريد*
1.0	ITU-T X.1604	2020-03-26	17	11.1002/1000/14093

مصطلحات أساسية

سحابية، الشبكة كخدمة، متطلبات الأمن.

* 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.1604

متطلبات أمن الشبكة كخدمة (NaaS) في الحوسبة السحابية

1 مجال التطبيق

تحلل هذه التوصية التهديدات والتحديات الأمنية التي تواجهها الشبكة كخدمة (NaaS) في الحوسبة السحابية وتحدد متطلبات الأمن للشبكة كخدمة في تطبيقات الشبكة كخدمة وجوانب منصات الشبكة كخدمة وتوصيلية الشبكة كخدمة استناداً إلى أنواع القدرات السحابية المقابلة.

2 المراجع

يتضمن ما يلي من توصيات قطاع تقييس الاتصالات في الاتحاد الدولي للاتصالات وغيرها من المراجع أحكاماً تندرج، من خلال الإحالة إليها في النص الحالي، في عِداد أحكام التوصية الحالية. وعند نشر التوصية الحالية كانت الطبعات المذكورة من المراجع المعنية سارية المفعول. لكن لمّا كانت جميع التوصيات وغيرها من المراجع تخضع لعمليات مراجعة فيوصى بأن يدرس من يطبّقون التوصية الحالية إمكانية تطبيق أحدث طبعة من التوصيات وسائر المراجع المذكورة أدناه. وتُنشر بانتظام قائمة بتوصيات قطاع تقييس الاتصالات السارية. والإشارة إلى وثيقة ما في هذه التوصية، لا يضفي على الوثيقة في حد ذاتها صفة التوصية.

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

[ITU-T Y.3500] التوصية ITU-T Y.3500 (2014) | ISO/IEC 17788:2014، *تكنولوجيا المعلومات – الحوسبة السحابية – نظرة عامة ومفردات*.

[ITU-T Y.3512] التوصية ITU-T Y.3512 (2014)، *الحوسبة السحابية – المتطلبات الوظيفية للشبكة كخدمة*.

3 التعاريف

1.3 المصطلحات المعرَّفة في وثائق أخرى

تستعمل هذه التوصية المصطلحات التالية المعرفة في وثائق أخرى:

1.1.3 التحكم في النفاذ (access control) [b-ITU-T X.800]: منع استخدام غير مرخص به لمورد ما، بما في ذلك منع استخدام مورد بطريقة غير مرخص بها.

2.1.3 الاستيقان (authentication) [b-ISO/IEC 18014-2]: توفير الثقة في هوية كيان.

3.1.3 التخويل (authorization) [b-ITU-T X.1251]: الغرض من خدمة التخويل هو اتخاذ القرارات فيما يتعلق بحقوق نفاذ المستعمل، وإنفاذ قرارات التخويل طبقاً لامتيازات المستعمل. ويُعد التخويل خدمة اختيارية لا تُقدم إلا عند الحاجة للتحكم بالنفاذ إلى الموارد على أساس حقوق المستعمل.

4.1.3 السرية (confidentiality) [b-ITU-T X.800]: خاصية عدم إتاحة المعلومات أو الكشف عنها لأشخاص غير مخوَّلين أو لكيانات، أو عمليات غير مُخَوَّلَة.

5.1.3 سلامة البيانات (data integrity) [b-ITU-T X.800]: خاصية بقاء البيانات على حالتها دون أن يطرأ عليها تغيير أو تلف بطريقة غير مرخص بها.

6.1.3 جدار الحماية (firewall) [b-ISO/IEC 27033-1]: نوع من الحواجز الأمنية يوضع بين البيئات الشبكية. يتألف من جهاز مكرس أو مجموعة من العديد من المكونات والتقنيات – تمر من خلاله كل الحركة العابرة من بيئة شبكية لأخرى، والعكس، ولا يسمح بمرور إلا الحركة المخوَّلة التي تحددها السياسات الأمنية المحلية.

7.1.3 نظام كشف الاقتحام (intrusion detection system) [b-ISO/IEC 27039]: أنظمة معلومات تستخدم للكشف عن محاولة اقتحام أو عن الاقتحام أثناء حدوثه أو بعد حدوثه.

8.1.3 مفتاح (key) [b-ITU-T X.800]: متوالية رموز تتحكم في عمليات التشفير وفك التشفير.

9.1.3 إدارة مفاتيح (key management) [b-ITU-T X.800]: توليد المفاتيح وتخزينها وتوزيعها وإلغاؤها وأرشفتها وتطبيقها طبقاً لسياسة الأمن.

10.1.3 شهادة المفتاح العمومي (public-key certificate) (PKC) [b-ITU-T X.509]: المفتاح العمومي لكيان، مصحوباً ببعض المعلومات الأخرى التي أصبحت غير قابلة للتزوير، عن طريق توقيع رقمي يستعمل فيه المفتاح الخاص الذي تصدره سلطة إصدار الشهادة.

11.1.3 تهديد (threat) [b-ISO/IEC 27000]: سبب محتمل لحادث غير مرغوب قد يُلحق ضرراً بالنظام أو المنظمة.

2.3 مصطلحات معرّفة في هذه التوصية

لا توجد.

4 الاختصارات والأسماء المختصرة

تستخدم هذه التوصية المختصرات والأسماء المختصرة التالية:

BoD عرض نطاق حسب الطلب *(Bandwidth on Demand)*

CSC عميل الخدمة السحابية *(Cloud Service Customer)*

CSP مورد الخدمة السحابية *(Cloud Service Provider)*

DDoS رفض الخدمة الموزّع *(Distributed Denial of Service)*

DoS رفض الخدمة *(Denial of Service)*

NaaS الشبكات كخدمة *(Network as a Service)*

SNMP بروتوكول بسيط لإدارة الشبكة *(Simple Network Management Protocol)*

vCDN شبكة توصيل المحتوى الافتراضية *(virtual content delivery network)*

vEPC شبكة رزم أساسية متطورة ذات طابع افتراضي *(virtualised Evolved Packet Core)*

vFW جدار حماية افتراضي *(virtual Firewall)*

VPN شبكة خاصة افتراضية *(Virtual Private Network)*

5 الاصطلاحات

يتعين فهم المصطلحات الأساسية التالية في هذه التوصية على النحو التالي:

"**يجب**" تدل على متطلَّب إلزامي يجب التقيّد به بصرامة، ولا يُسمح بأي انحراف عنه في حال ادعاء الامتثال لهذه التوصية.

"**يوصى**" كلمة تدل على متطلب يوصى به لكنه غير إلزامي بالمطلق. وبالتالي لا يتعين توفر هذا المتطلب لزعم الامتثال.

"**يحظر**" تدل على متطلب إلزامي يجب التقيد به بصرامة ولا يسمح بأي انحراف عنه في حال زعم الامتثال لهذه التوصية.

"**من الجائز**" تدل على مطلب اختياري مسموح به دون أن ينطوي على أي توصية به. ولا يرمي هذا المصطلح إلى إلزام تطبيق البائع بتوفير هذا الخيار الذي يمكن أن يوفره مشغل الشبكة/مورد الخدمة اختيارياً. وبالأحرى، فإن البائع يمكنه إدراج هذه الخاصية اختيارياً ويدعى إلى الامتثال لهذه التوصية في نفس الوقت.

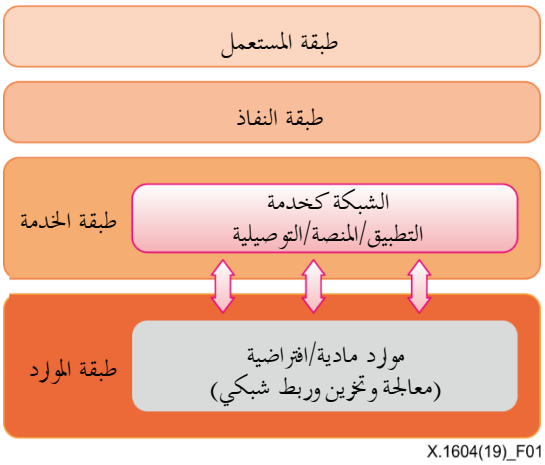
6 نظرة عامة

طبقاً للتوصية [ITU-T Y.3500]، فئة الخدمة السحابية هي مجموعة من الخدمات السحابية التي تقترح مجموعة مشتركة من الكميات. والشبكة كخدمة (NaaS) هي واحدة من فئات الخدمات السحابية تكون فيها القدرة التي يزود بها عميل الخدمة السحابية (CSC) هي توصيلية النقل وأي قدرات شبكية ذات صلة.

وكما هو محدد في التوصية [ITU-T Y.3512]، فإن خدمات الشبكة كخدمة يمكن أن توفر أي قدرة من القدرات السحابية الثلاث التالية: خدمة تطبيق NaaS، وخدمة منصة NaaS وخدمة توصيلية NaaS.

- **خدمة تطبيق NaaS** تزود العميل CSC بتطبيق شبكة سحابية مثل مسير افتراضي وشبكة vCDN وشبكة vEPC وجدار حماية افتراضي (vFW).
- **خدمة منصة NaaS** تزود العميل CSC بمنصة شبكية توفر بيئة قابلة للبرمجة لوظائف الشبكة.
- **خدمة توصيلية NaaS** توفر عملاء الخدمة السحابية وتستعمل موارد التوصيلية الشبكية مثل الشبكة الخاصة الافتراضية (VPN) المرنة والموسعة وعرض النطاق حسب الطلب (BoD) وما إلى ذلك.

ويمكن وصف المفهوم رفيع المستوى للشبكة NaaS كما هو موضح في الشكل 1:



الشكل 1 – مفهوم رفيع المستوى للشبكة كخدمة

وباستخدام هذه الأنواع الثلاثة من خدمات الربط الشبكي، يمكن للشبكة كخدمة أن توفر وظائف الشبكة في الحوسبة السحابية بما في ذلك: تنسيق حوسبة وتخزين الطابع الافتراضي مع قدرات الشبكة والتحكم المنسق في تكنولوجيات الشبكة غير المتجانسة وإعادة التشكيل حسب الطلب.

ومن جهة أخرى، تواجه الشبكة كخدمة أيضاً العديد من التحديات الأمنية:

- **التهديدات والتحديات الأمنية على تطبيق الشبكة كخدمة:** تتمثل خدمة تطبيق الشبكة كخدمة في توفير تطبيقات الشبكة الافتراضية لعميل الخدمة السحابية عن طريق مورد الخدمة السحابية، مثل جدار الحماية الافتراضي والمسير الافتراضي وشبكة توصيل المحتوى الافتراضية (vCDN) وما إلى ذلك. وتواجه أي خدمة لتطبيق الشبكة كخدمة تحديات أمنية تتعلق بمواطن الضعف الأمنية للتطبيق ومخاطر أمنية على إضفاء الطابع الافتراضي على الشبكة والاستعمال المشترك لأجهزة الشبكة المادية وما إلى ذلك.
- **التهديدات والتحديات الأمنية على منصة الشبكة كخدمة:** تتمثل خدمة منصة الشبكة كخدمة في توفير بيئات برمجية ومنصة لإدارة ونشر وتشغيل تطبيقات الشبكة لعميل خدمة سحابية بواسطة مورد خدمة سحابية. وتشمل التحديات الأمنية على منصة الشبكة كخدمة، على سبيل الذكر وليس الحصر، هجمات رفض الخدمة على منصات الشبكة ومواطن الضعف الأمنية لأنظمة التشغيل وانهيار التحكم في النفاذ وما إلى ذلك.
- **التهديدات والتحديات الأمنية على توصيلية الشبكة كخدمة:** تتمثل خدمة توصيلية الشبكة كخدمة في توفير التوصيل الشبكي لعميل الخدمة السحابية بواسطة مورد الخدمة السحابية، مثل الشبكة الخاصة الافتراضية وعرض النطاق حسب الطلب وما إلى ذلك. وتتسبب المشكلة الأمنية لخدمة التوصيلية في مخاطر ليس على خدمات الشبكة كخدمة فحسب، ولكن على موارد الحوسبة الأخرى أيضاً وعلى بيانات عميل الخدمة السحابية. وتشمل التحديات الأمنية أمام خدمة توصيلية الشبكة كخدمة على سبيل الذكر وليس الحصر التنصت على الشبكة وهجمات الاعتراض لوسيط وما إلى ذلك.

وتحلل هذه التوصية متطلبات الأمن للشبكة كخدمة في الحوسبة السحابية، بما في ذلك تطبيق الشبكة كخدمة ومنصة الشبكة كخدمة وتوصيلية الشبكة كخدمة.

7 التهديدات والتحديات الأمنية للشبكة كخدمة في الحوسبة السحابية

توثق الفقرتان 7 و8 بالتوصية [ITU-T X.1601] التهديدات والتحديات الأمنية لعميل الخدمة السحابية ومورد الخدمة السحابية في الحوسبة السحابية، على التوالي. والشبكة كخدمة في الحوسبة السحابية تواجه أيضاً تهديدات وتحديات أمنية مماثلة لتلك المعرفة في التوصية [ITU-T X.1601] كما هو مبين أدناه:

أ) مواطن ضعف النظام؛

ب) فقدان وتسرب البيانات؛

ج) نفاذ غير آمن إلى الخدمة؛

د) نفاذ إدارة غير مخوَّلة؛

هـ) تهديدات داخلية؛

و) فقدان الثقة؛

ز) غياب الإدارة؛

ح) غياب السرية؛

ط) عدم تيسر الخدمة؛

ي) بيئة مشتركة.

وبالنسبة لكل قدرة سحابية، تواجه الشبكة كخدمة في الحوسبة السحابية تهديدات وتحديات أمنية خاصة.

1.7 التهديدات والتحديات الأمنية لتطبيق الشبكة كخدمة

أ) مواطن ضعف الشبكة والنظام: يمكن للمهاجمين استغلال مواطن الضعف الأمنية المحتملة لتطبيق الشبكة كخدمة. ويمكن للعيوب التقنية الناتجة عن إضفاء الطابع الافتراضي على تطبيق الشبكة كخدمة أن تتسبب في العديد من المخاطر الأمنية؛ كما أن تكنولوجيات التشغيل والصيانة غير المكتملة يمكن أن تنتج مخاطر أكثر خطورة.

ب) الاستعمال المشترك للأجهزة الشبكية المادية: عند الاشتراك في استعمال الأجهزة الشبكة المادية، يمكن فقدان البيانات الموجودة على أحد الأجهزة المتقاسمة أو تسربها أو إساءة استعمالها.

ج) النفاذ غير المؤمن: يمكن للنفاذ غير المؤمن إلى تطبيق الشبكة كخدمة أن يتسبب في فقدان بيانات التطبيق أو تسربها أو إساءة استعمالها.

د) نفاذ إدارة غير مخوَّلة: يمكن لنفاذ إدارة غير مخوَّلة إلى تطبيق الشبكة كخدمة أن يتسبب في فقدان البيانات.

هـ) عدم تيسر التطبيق: يمكن الهجوم على تطبيق الشبكة كخدمة بهجمات رفض الخدمة (DoS) أو الرفض الموزع للخدمة (DDoS)؛ كما يمكن لهذا الهجوم أن يتسبب في إلحاق الضرر بمعدات العتاد مع فقدان البيانات أو تدميرها.

2.7 التهديدات والتحديات الأمنية لمنصة الشبكة كخدمة

أ) هجمات رفض الخدمة على منصة الشبكة: عندما تتعرض منصة أو أكثر لهجمات رفض الخدمة (DoS)، فإن المنصة والمنصات الافتراضية الأخرى لا يمكنها الاستجابة نظراً للاستهلاك العابر للوحدة المعالجة المركزية (CPU) والذاكرة.

ب) مواطن الضعف الأمنية لنظام التشغيل: يمكن فقدان البيانات الموجودة على منصات الشبكة كخدمة؛ كما يمكن لمواطن الضعف الأمنية لأنظمة التشغيل أن تتسبب في انتشار الفيروسات والمخاطر الأمنية الخطيرة الأخرى.

ج) انقطاع التحكم في النفاذ: يمكن لانقطاع التحكم في النفاذ أن يتسبب في فقدان البيانات أو تسربها أو إساءة استعمالها.

د) عدم تيسر منصة الشبكة: يمكن لعدم تيسر منصة الشبكة كخدمة أن يؤدي إلى عدم تيسر خدمات الشبكة كخدمة، لذا، يمكن لتطبيقات الشبكة كخدمة وتوصيلية الشبكة كخدمة ألا تعمل هي الأخرى.

هـ) نفاذ الإدارة غير المخوَّل به: يمكن لنفاذ الإدارة غير المخوَّل به إلى منصة لشبكة كخدمة أن يؤدي إلى فقدان البيانات أو تسربها أو إساءة استعمالها. فعلى سبيل المثال، قد يستغل مهاجمون موطن ضعف في النظام للحصول على نفاذ إدارة غير مخوَّل به إلى منصة الشبكة كخدمة وتعديل عنوان بروتوكول الإنترنت لمقصد جمع البيانات إلى عنوان المهاجم.

و) التهديدات الداخلية للموظفين: إذا كان عميل خدمة الشبكة كخدمة شركة أو منظمة، وليس شخصاً، فإن موظفي الشركة يتشاركون في كلمات المرور "الإدارة"، وكذلك مورد خدمة الشبكة كخدمة. ووجود مستعملين لا مبالين أو غير مدربين بالقدر الكافي (أو أفراد العائلة في حالة العميل)، أو الأفعال الخبيثة التي يقوم بها بعض الموظفين الناقمين، هي أمور تشكل دائماً تهديداً كبيراً.

3.7 التهديدات والتحديات الأمنية لتوصيلية الشبكة كخدمة

أ) التنصت: يمكن للمهاجمين التنصت على بيانات التوصيل وبيانات الإرسال.

ب) هجمات التوصيلات الشبكية: يمكن أن تحدث هذه الهجمات أثناء توصيل الشبكة مثل هجمات الأطراف الوسيطة وهجمات رفض الخدمة وما إلى ذلك.

ج) فقدان البيانات وتسربها: عند استعمال الخدمات NaaS، يستعمل عملاء NaaS عادةً الشبكة المقدمة من موردي الخدمات NaaS لنقل البيانات. ويمكن لهذه البيانات أن تتضمن معلومات خصوصية شخصية وأسرار تجارية وقضايا سياسية. من هنا، فإن تسرب البيانات يمثل تهديداً خطيراً لمستعملي الخدمات NaaS.

د) الانتحال: يمكن لمهاجمين انتحال صفة نظام إدارة أو مخدِّم تخزين البيانات لدى خدمة NaaS للحوسبة السحابية، والتسبب بفقدان بيانات التوصيل أو بيانات الإرسال.

هـ) العبث والاعتراض: يرجح أن تتسبب معدات الشبكة التالفة وعمليات الاقتحام التي يقوم بها القراصنة وإفلاس مورد الخدمة في فقدان البيانات وتعذر استعادتها. وإلى جانب ذلك، يمكن للقراصنة التلاعب بالبيانات إذا نجحوا في الدخول إلى الشبكة.

و) النفاذ غير المؤمن إلى الشبكة: يمكن للنفاذ غير المؤمن إلى الشبكة أن يتسبب في فقدان بيانات التوصيل أو بيانات الإرسال أو تسربها أو إساءة استعمالها.

ز) الاستيقان غير المؤمن للهوية: يمكن للاستيقان غير المؤمن للهوية أن يتسبب في فقدان بيانات التوصيل أو بيانات الإرسال أو تسربها أو إساءة استعمالها.

ح) عدم تيسر الشبكة: يمكن تعرض شبكة توصيلية الخدمة NaaS لهجمات رفض الخدمة أو هجمات رفض الخدمة الموزع، كما يمكن لهذه الخدمات أن تؤدي إلى إتلاف لخدمات الخدمة NaaS في الحوسبة السحابية.

ط) التوصل إلى موطن ضعف في السطح البيني: يمكن للمهاجمين استخدام حيازة بيانات المراقبة لاستغلال مواطن ضعف السطوح البينية.

ي) نفاذ إدارة غير مخوَّلة: يمكن لنفاذ الإدارة غير المخوَّلة إلى نظام توصيلية الخدمة NaaS إلى فقدان بيانات الإرسال.

8 المتطلبات الأمنية لتطبيق الشبكة كخدمة

يحدد هذا القسم المتطلبات الأمنية للشبكة كخدمة الحوسبة السحابية.

1.8 المتطلبات الأمنية لتطبيق الشبكة كخدمة

تشمل المتطلبات الأمنية لتطبيق الشبكة كخدمة ما يلي:

أ) ضرورة الحفاظ على سلامة ودقة بيانات تطبيق الشبكة كخدمة.

ب) يوصى بتوفير أساليب للتحكم في النفاذ إلى بيانات تطبيق الشبكة كخدمة مثل القوائم البيضاء والقوائم السوداء وما إلى ذلك.

ج) يوصى بأن يوفر مورد الخدمة السحابية الأساليب المناسبة للتحكم في النفاذ إلى عميل الخدمة السحابية مثل القوائم البيضاء/السوداء والحسابات وكلمات السر وما إلى ذلك لمنع نفاذ المستعملين غير المخوَّلين إلى النظام أو إلى البيانات. وترد الحلول الشائعة للتحكم في النفاذ في الحوسبة السحابية في التوصية [ITU-T X.1601].

د) ضرورة أن يدعم مورد الخدمة السحابية تسجيل وتدقيق استعمال تطبيق الشبكة كخدمة.

هـ) ضرورة أن يدعم مورد الخدمة السحابية الدفاعات ضد مواطن ضعف نظام تطبيق الشبكة كخدمة؛ حيث يمكن لمورد الخدمة السحابية أن يستخدم، على سبيل الثمال، أساليب اختبار الاختراق لمنع مواطن ضعف نظام تطبيق الشبكة كخدمة.

و) ضرورة توفير مورد الخدمة السحابية أساليب توفير الرديف لمنع فقدان بيانات تطبيق الشبكة كخدمة، مثل توفير الرديف باستخدام الأقراص المادية وأساليب التخزين الموزع للبيانات وما إلى ذلك. ويرد وصف الأساليب الشائعة لتوفير الرديف في التوصية [ITU-T X.1601].

ويعرض الجدول 8-1 تقابلاً موجزاً بين التهديدات الأمنية لتطبيق الشبكة كخدمة والمتطلبات الأمنية.

الجدول 8-1: تطبيق الشبكة كخدمة: التهديدات الأمنية وما يقابلها من المتطلبات الأمنية

التهديدات الأمنية	المتطلبات الأمنية
مواطن الضعف الأمنية للتطبيق	ب)، د)، هـ)، و)
المخاطر الأمنية لإضفاء الطابع الافتراضي على الشبكة	أ)، ب)، ج)، د)، و)
الاستعمال المشترك للأجهزة المادية للشبكة	أ)، ب)، ج)، د)، و)
النفاذ غير المؤمن	ب)، ج)، د)، هـ)، و)
نفاذ إدارة غير مخوَّلة	ب)، ج)، د)، و)
مواطن ضعف التطبيق	د)، هـ)، و)

2.8 المتطلبات الأمنية لمنصة الشبكة كخدمة

تشمل المتطلبات الأمنية لمنصة الشبكة كخدمة ما يلي:

أ) ضرورة الحفاظ على سلامة ودقة بيانات منصة الشبكة كخدمة.

ب) يوصى بتوفير أساليب للتحكم في النفاذ إلى بيانات منصة الشبكة كخدمة مثل القوائم البيضاء والقوائم السوداء وما إلى ذلك.

ج) يوصى بأن يوفر مورد الخدمة السحابية الأساليب المناسبة للتحكم في النفاذ إلى عميل الخدمة السحابية مثل القوائم البيضاء/السوداء والحسابات وكلمات السر وما إلى ذلك لمنع نفاذ المستعملين غير المخوَّلين إلى النظام أو إلى البيانات. ويرد وصف الحلول الشائعة للتحكم في النفاذ في الحوسبة السحابية في التوصية [ITU-T X.1601].

د) ضرورة أن يدعم مورد الخدمة السحابية تسجيل وتدقيق استعمال منصة الشبكة كخدمة.

هـ) ضرورة أن يدعم مورد الخدمة السحابية الدفاعات ضد مواطن ضعف نظام منصة الشبكة كخدمة؛ حيث ينبغي، على سبيل المثال، أن يمنع مورد الخدمة السحابية فقدان البيانات وتسربها على منصة الشبكة كخدمة.

و) ضرورة توفير مورد الخدمة السحابية أساليب توفير الرديف لمنع فقدان بيانات منصة الشبكة كخدمة، مثل توفير الرديف باستخدام الأقراص المادية وأساليب التخزين الموزع للبيانات وما إلى ذلك. وترد الأساليب الشائعة لتوفير الرديف في التوصية [ITU-T X.1601].

ويعرض الجدول 8-2 تقابلاً موجزاً بين التهديدات الأمنية لمنصة الشبكة كخدمة والمتطلبات الأمنية.

الجدول 8-2: منصة الشبكة كخدمة: التهديدات الأمنية وما يقابلها من المتطلبات الأمنية

التهديدات الأمنية	المتطلبات الأمنية
هجمات رفض الخدمة على منصة الشبكة	أ)، ب)، ج)، د)، هـ)، و)
مواطن الضعف الأمنية لنظام التشغيل	أ)، ب)، د)، هـ)، و)
تحكم فاشل في النفاذ	أ)، ب)، ج)، د)، هـ)، و)
مواطن ضعف منصة الشبكة	أ)، د)، هـ)، و)
نفاذ إدارة غير مخوَّلة	ب)، ج)، د)، و)
التهديدات الداخلية للموظفين	ب)، د)، و)

3.8 المتطلبات الأمنية لتوصيلية الشبكة كخدمة

تشمل المتطلبات الأمنية لتوصيلية الشبكة كخدمة ما يلي:

أ) ضرورة الحفاظ على سلامة ودقة بيانات توصيلية الشبكة كخدمة.

ب) يوصى بتوفير أساليب للتحكم في النفاذ إلى بيانات توصيلية الشبكة كخدمة مثل القوائم البيضاء والقوائم السوداء وما إلى ذلك.

ج) يوصى بتوفير أساليب تجفيرية لضمان أمن بيانات التوصيل والإرسال.

د) يوصى باستخدام بروتوكولات شبكية قياسية بين الموارد السحابية ومخدمات توصيلية الشبكة كخدمة مثل البروتوكول البسيط لإدارة الشبكة (SNMP) أو غيره من البروتوكولات الشبكية القياسية.

هـ) يوصى بأن يوفر مورد الخدمة السحابية الأساليب المناسبة للتحكم في النفاذ إلى عميل الخدمة السحابية مثل القوائم البيضاء/السوداء والحسابات وكلمات السر وما إلى ذلك لمنع نفاذ المستعملين غير المخوَّلين إلى النظام أو إلى البيانات. وترد الحلول الشائعة للتحكم في النفاذ في الحوسبة السحابية في التوصية [b-ITU-T X.1601].

و) ضرورة أن يدعم مورد الخدمة السحابية تسجيل وتدقيق استعمال توصيلية الشبكة كخدمة.

ز) ضرورة تنفيذ مورد الخدمة السحابية لأساليب للاستيقان لحماية النفاذ إلى بيانات توصيلية الشبكة كخدمة مثل الاستيقان بعاملين أو أي أساليب أخرى. ويرد وصف أساليب الاستيقان الشائعة للحوسبة السحابية في التوصية [ITU-T X.1601].

ح) ضرورة دعم مورد الخدمة السحابية للدفاعات ضد مواطن ضعف نظام توصيلية الشبكة كخدمة. فعلى سبيل المثال، يمكن لمورد الخدمة السحابية أن يستخدم أساليب اختبار الاختراق لمنع مواطن ضعف نظام توصيلية الشبكة كخدمة.

ويعرض الجدول 8-3 تقابلاً موجزاً بين التهديدات الأمنية والمتطلبات الأمنية لتوصيلية الشبكة كخدمة.

الجدول 8-3: توصيلية الشبكة كخدمة: التهديدات الأمنية وما يقابلها من المتطلبات الأمنية

التهديدات الأمنية	المتطلبات الأمنية
التنصت	ب)، ج)، د)، هـ)، و)، ز)، ح)
الهجمات على التوصيلات الشبكية	د)، و)، ح)
فقدان البيانات وتسربها	أ)، ب)، ج)، د)، هـ)، و)، ز)، ح)
الانتحال	أ)، ب)، د)، هـ)، و)، ز)، ح)
العبث والاعتراض	أ)، ب)، ج)، د)، هـ)، و)، ز)، ح)
النفاذ إلى الخدمة غير المؤمن	ب)، ج)، د)، هـ)، و)، ز)، ح)
الاستيقان غير المؤمن للهوية	ب)، ج)، هـ)، و)، ز)، ح)
مواطن ضعف الشبكة	د)، و)، ح)
موطن ضعف السطح البيني للتحصيل	أ)، ب)، ج)، د)، و)، ح)
نفاذ إدارة غير مخوَّلة	ج)، و)، ز)

بيبليوغرافيا

[b-ITU-T E.409] Recommendation ITU-T E.409 (2004), *Incident organization and security incident handling: Guidelines for telecommunication organizations.*

[b-ITU-T X.509] Recommendation ITU-T X.509 (2019) | ISO/IEC 9594-8:2020, *Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks*.

[b-ITU-T X.800] Recommendation ITU-T X.800 (1991) | ISO/IEC 7498-2:1989, *Security architecture for Open Systems Interconnection for CCITT applications*.

[b-ITU-T X.810] Recommendation ITU-T X.810 | ISO/IEC 10181-1 :1995, *Information technology – Open System Interconnection – Security frameworks for open system: Overview.*

[b-ITU-T X.1251] التوصية ITU-T X.1215 (2019)، *حالات الاستعمال المتعلقة بلغة التعبير المهيكل عن معلومات التهديدات.*

[b-ITU-T Y.3502] Recommendation ITU-T Y.3502 | ISO/IEC 17789:2014, *Information technology – Cloud computing – Reference architecture.*

[b-ISO/IEC 18014-2]: المعيار ISO/IEC 18014-2:2009 *تكنولوجيا المعلومات – تقنيات الأمن – خدمات خاتم التوقيت – الجزء 2: آليات توليد الأذنات المستقلة.*

[b-ISO/IEC 19440] ISO/IEC 19440: 2007, *Enterprise integration – Constructs for enterprise modelling.*

[b-ISO/IEC 19944] ISO/IEC 19944:2017, *Information technology – Cloud services and devices: data flow, data categories and data use.*

[b-ISO/IEC 20000-1] ISO/IEC 20000-1:2011, *Information technology –Service management – Part1: Service management system requirements.*

[b-ISO/IEC 27000] ISO/IEC 27000:2018, *Information technology –Security techniques – Information security management systems – Overview and vocabulary.*

[b-ISO/IEC 27033-1] ISO/IEC 27033-1:2015, *Information technology – Security techniques – Network security – Part 1: Overview and concepts*.

[b-ISO/IEC 27039] ISO/IEC 27039:2015, *Information technology – Security techniques – Selection, deployment and operations of intrusion detection and prevention systems (IDPS).*

[b-ISO/IEC 27729] ISO/IEC 27729:2012, *Information and documentation – International standard name identifier (ISNI).*

[b-ISO/IEC 29100] ISO/IEC 29100:2011, *Information technology –Security techniques –Privacy framework.*

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، 2020