التـوصيــة

ITU-T X.1644 (03/2023)

السلسلة X: شبكات البيانات والاتصالات بين الأنظمة المفتوحة ومسائل الأمن

أمن الحوسبة السحابية – أفضل الممارسات ومبادئ توجيهية بشأن أمن الحوسبة السحابية

مبادئ توجيهية أمنية بشأن الحوسبة السحابية الموزَّعة

توصيات السلسلة X الصادرة عن قطاع تقييس الاتصالات

شبكات البيانات والاتصالات بين الأنظمة المفتوحة ومسائل الأمن

الشبكات العمومية للبيانات	X.1–X.199
التوصيل البيني للأنظمة المفتوحة	X.200–X.299
التشغيل البيني للشبكات	X.300–X.399
أنظمة معالجة الرسائل	X.400–X.499
الدليل	X.500–X.599
التشغيل البيني لأنظمة التوصيل OSI ومظاهر النظام	X.600–X.699
إدارة التوصيل البيني للأنظمة المفتوحة (OSI)	X.700–X.799
الأمن	X.800–X.849
تطبيقات التوصيل البيني للأنظمة المفتوحة (OSI)	X.850–X.899
المعالجة الموزعة المفتوحة	X.900–X.999
أمن المعلومات والشبكات	
الجوانب العامة للأمن	X.1000–X.1029
أمن الشبكة	X.1030–X.1049
إدارة الأمن	X.1050–X.1069
القياس الحيوي عن بُعد	X.1080–X.1099
تطبيقات وخدمات آمنة (1)	
أمن البث المتعدد	X.1100–X.1109
أمن الشبكة المحلية	X.1110–X.1119
أمن الخدمات المتنقلة	X.1120–X.1139
أمن الويب (1)	X.1140–X.1149
أمن التطبيقات (1)	X.1150–X.1159
الأمن بين جهتين نظيرتين	X.1160–X.1169
أمن معرفات الهوية عبر الشبكات	X.1170–X.1179
أمن التلفزيون القائم على بروتوكول الإنترنت	X.1180–X.1199
أمن الفضاء السيبراني	
الأمن السيبراني	X.1200–X.1229
مكافحة الرسائل الاقتحامية	X.1230–X.1249
إدارة الهوية	X.1250–X.1279
تطبيقات وخدمات آمنة (2)	
اتصالات الطوارئ	X.1300–X.1309
أمن شبكات المحاسيس واسعة الانتشار	X.1310–X.1319
أمن شبكة الكهرباء الذكية	X.1330–X.1339
البريد المعتمد	X.1340–X.1349
أمن إنترنت الأشياء (IoT)	X.1350–X.1369
أمن أنظمة النقل الذكية (ITS)	X.1370–X.1399
أمن سجل الحسابات الموزع	X.1400–X.1429
أمن التطبيقات (2)	X.1450–X.1459
أمن شبكة الويب (2)	X.1470–X.1489
تبادل معلومات الأمن السيبراني	
نظرة عامة عن الأمن السيبراني	X.1500–X.1519
تبادل المعلومات عن مواطن الضعف/الحالة	X.1520–X.1539
تبادل المعلومات عن الأحداث/الأحداث العارضة/المعلومات الحدسية	X.1540–X.1549
تبادل المعلومات عن السياسات	X.1550–X.1559
طلب المعلومات الحدسية والمعلومات الأخرى	X.1560–X.1569
تعرف الهوية والاكتشاف	X.1570–X.1579
التبادل المضمون	X.1580–X.1589
الدفاع السيبراني	X.1590–X.1599
أمن الحوسبة السحابية	
نظرة عامة على أمن الحوسبة السحابية	X.1600–X.1601
تصميم أمن الحوسبة السحابية	X.1602–X.1639
أفضل الممارسات ومبادئ توجيهية بشأن أمن الحوسبة السحابية	**X.1640–X.1659**
تنفيذ أمن الحوسبة السحابية	X.1660–X.1679
أمن أشكال أخرى للحوسبة السحابية	X.1680–X.1699
الاتصالات الكمومية	
المصطلحات	X.1700–X.1701
مولّد الأعداد العشوائية الكمومية	X.1702–X.1709
إطار أمن شبكات توزيع المفاتيح الكمومية	X.1710–X.1711
تصميم أمن شبكات توزيع المفاتيح الكمومية	X.1712–X.1719
تقنيات أمن شبكات توزيع المفاتيح الكمومية	X.1720–X.1729
أمن البيانات	
أمن البيانات الضخمة	X.1750–X.1759
حماية البيانات	X.1770–X.1789
أمن شبكات الاتصالات المتنقلة الدولية-2020	X.1800–X.1819

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

التوصية ITU-T X.1644

مبادئ توجيهية أمنية بشأن الحوسبة السحابية الموزَّعة

ملخص

تُحلل التوصية ITU-T X.1644 التهديدات والتحديات الأمنية التي تتعرض لها الحوسبة السحابية الموزعة، وتقترح مبادئ توجيهية أمنية للتصدي لما قد يستهدف الحوسبة السحابية الموزعة من تهديدات، وتشمل المبادئ المقترحة مبادئ توجيهية أمنية تتعلق بالحوسبة السحابية الأساسية والحوسبة السحابية الإقليمية وحوسبة الحافة السحابية.

التسلسل التاريخي

الطبعة	التوصية	تاريخ الموافقة	لجنة الدراسات	معرف الهوية الفريد*
1.0	ITU-T X.1644	2023-03-03	17	11.1002/1000/15112

مصطلحات أساسية

الحوسبة السحابية، الحوسبة السحابية الموزَّعة، مبادئ توجيهية 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 هو وكالة الأمم المتحدة المتخصصة 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 اختراع/حقوق تأليف برمجيات 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 قواعد البيانات المناسبة لقطاع تقييس الاتصالات المتاحة من خلال الموقع الإلكتروني لقطاع تقييس الاتصالات في العنوان http://www.itu.int/ITU-T/ipr/.

جدول المحتويات

الصفحة

التوصية ITU-T X.1644

مبادئ توجيهية أمنية بشأن الحوسبة السحابية الموزَّعة

1 مجال التطبيق

تُحلل هذه التوصية التهديدات الأمنية التي قد تتعرض لها الحوسبة السحابية الموزعة وتقدم مبادئ توجيهية أمنية لها.

2 المراجع

تتضمن التوصيات التالية لقطاع تقييس الاتصالات وغيرها من المراجع أحكاماً تشكل من خلال الإشارة إليها في هذا النص جزءاً لا يتجزأ من هذه التوصية. وقد كانت جميع الطبعات المذكورة سارية الصلاحية في وقت النشر. ولما كانت جميع التوصيات والمراجع الأخرى تخضع للمراجَعة، يُشجع جميع مستعملي هذه التوصية على بحث إمكانية تطبيق أحدث طبعة للتوصيات والمراجع الأخرى الواردة أدناه. وتُنشر بانتظام قائمة توصيات قطاع تقييس الاتصالات السارية الصلاحية. والإشارة إلى وثيقة ما في هذه التوصية لا يضفي على الوثيقة في حد ذاتها صفة التوصية.

[ITU-T X.1408] التوصية ITU-T X.1408 (2021)، *التهديدات والمتطلبات الأمنية للنفاذ إلى البيانات وتقاسمها على أساس تكنولوجيا السجلات الموزَّعة*.

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

[ITU-T Y.3500] التوصية ITU-T Y.3500 (2014)، *تكنولوجيا المعلومات – الحوسبة السحابية –نظرة عامة ومفردات*.

[ITU-T Y.3508] التوصية ITU-T Y.3508 (2019)، *الحوسبة السحابية – نظرة عامة على الحوسبة السحابية الموزعة ومتطلباتها العامة*.

3 التعاريف

1.3 المصطلحات المعرَّفة في مراجع أخرى

تستخدم هذه التوصية المصطلحات التالية المعرَّفة في وثائق أخرى:

1.1.3 نوع قدرات الخدمة السحابية (cloud capabilities type) [ITU-T Y.3500]: هو تصنيف للوظائف التي توفرها خدمة سحابية إلى عميل الخدمة السحابية استناداً إلى الموارد المستعملة.

ملاحظة – أنواع قدرات الخدمة السحابية هي نوع قدرات التطبيقات، ونوع قدرات البنية التحتية، ونوع قدرات المنصة.

2.1.3 الحوسبة السحابية (cloud computing) [ITU-T Y.3500]: هي 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.

3.1.3 الخدمة السحابية (cloud service) [ITU-T Y.3500]: هي قدرة واحدة أو عدد أكبر من القدرات تُقدم عن طريق الحوسبة السحابية وتُلبى باستخدام سطح بيني معلن.

4.1.3 عميل الخدمة السحابية (cloud service customer) [ITU-T Y.3500]: هو طرف مرتبط بعلاقة تجارية لأغراض استخدام الخدمات السحابية.

ملاحظة – لا تستوجب العلاقة التجارية بالضرورة وجود اتفاقات مالية.

5.1.3 مقدم الخدمة السحابية (cloud service provider) [ITU-T Y.3500]: هو الطرف الذي يُتيح الخدمات السحابية.

6.1.3 حوسبة الحافة السحابية (edge cloud) [ITU-T Y.3508]: هي إحدى تكنولوجيات الحوسبة السحابية تُنشر عند حافة الشبكة، يَنفُذ إليها مستهلكو الخدمات السحابية (CSC) وتُفعِّل الخدمة السحابية بموارد صغيرة السِّعة.

ملاحظة 1 –الخدمات السحابية المفعَّلة على حوسبة الحافة السحابية هي خدمات سحابية خفيفة الوزن يقدمها أحد مقدمي الخدمات السحابية (CSP) تبعاً لفئاتها.

ملاحظة 2 – تشير الخدمة السحابية الخفيفة الوزن إلى الجزء الموجود في الخدمة السحابية الذي يُعيد تشكيل خصائصها الوظيفية ليتسنى إدماجها في حوسبة حافة سحابية مواردها صغيرة السِّعة كمحطة القاعدة والبوابة.

7.1.3 التهديد (threat) [ITU-T X.1408]: سبب محتمل لحادث غير مرغوب قد يُلحق ضرراً بالنظام أو المنظمة.

2.3 المصطلحات المعرفة في هذه التوصية

تعرّف هذه التوصية المصطلحات التالية:

1.2.3 الحوسبة السحابية الأساسية: هي مجموعة مركزية من الخدمات تشمل جميع الخدمات غير المقيَّدة جغرافياً، والخدمات غير المتأثرة بالكُمون، والخدمات ذات الاستخدام الكثيف للغاية للموارد الحاسوبية، وخدمات الدعم الاحتياطي والاستعادة، فضلاً عن الخدمات ذات مستوى الأمن العالي في شبكة الحوسبة السحابية.

2.2.3 الحوسبة السحابية الموزَّعة: هي امتداد للمفاهيم التقليدية للحوسبة السحابية، يزيد من توسيع نطاق قدرات الحوسبة السحابية ليصل به إلى حافة الشبكة.

3.2.3 الحوسبة السحابية الإقليمية: هي حوسبة سحابية أساسية تُنشر اختيارياً لضمان كفاءة التشكيل بين الحوسبة السحابية الأساسية وحوسبة الحافة السحابية بغرض تخفيض الحِمل على الحوسبة السحابية الأساسية.

4 الاختصارات والأسماء المختصرة

تستعمل هذه التوصية الاختصارات والأسماء المختصرة التالية:

API السطح البيني لبرمجة التطبيقات (*Application Service Interface*)

CC الحوسبة السحابية الأساسية (*Core Cloud*)

CSC مستهلك خدمة سحابية (*Cloud Service Customer*)

CSP مقدِّم خدمات سحابية (*Cloud Service Provider*)

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

DoS رفض الخدمة (*Denial of Service*)

EC حوسبة الحافة السحابية (*Edge Cloud*)

IoT إنترنت الأشياء (*Internet of Thing*)

OTA عبر الأثير (*Over-The-Air*)

REST نقل الحالة التمثيلية (*Representational State Transfer*)

TLS أمن طبقة النقل (*Transport Layer Security*)

VPN شبكة خاصة افتراضية (*Virtual Private Network*)

XML لغة الوسم القابلة للتوسيع (*Extensible Markup Language*)

XSS البرمجة النصية العابرة للمواقع (*Cross Site Scripting*)

5 الاصطلاحات

تستخدم هذه التوصية الاصطلاحين التاليين:

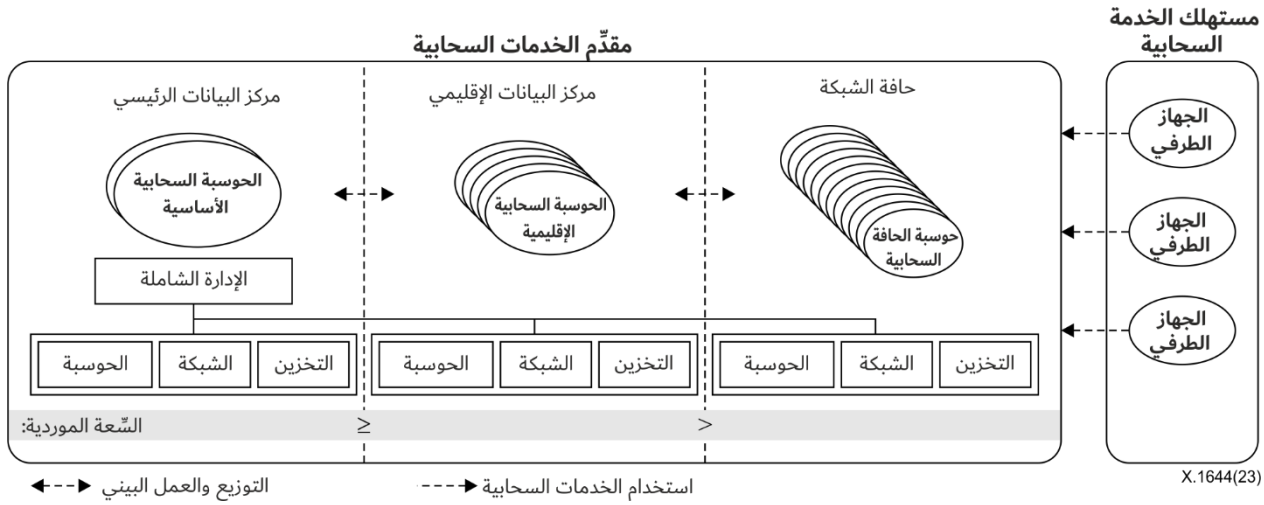
يدل الفعل "**يُشترط**" على متطلب يجب التقيد به تقيداً صارماً ولا يسمح بأي حياد عنه في حال ادعاء المطابقة لهذه التوصية.

ويدل الفعل "**يوصى**" على متطلب يوصى باستيفائه لكن لا يُشترط ذلك حتماً. وبالتالي، لا يُشترط استيفاء هذا المتطلب لادعاء المطابقة.

6 لمحة عامة

تنشأ تكنولوجيا الحوسبة السحابية الموزَّعة في الوقت الحاضر نظراً إلى تزايد عدد الخدمات الحساسة من حيث الكمون (كخدمات الفيديو وإنترنت الأشياء (IoT)) التي تلزمها سرعات استجابة أعلى كثيراً؛ فهي امتداد للحوسبة السحابية التقليدية يزيد من توسيع نطاق قدراتها ليصل به إلى حافة الشبكة. ويمكن للحوسبة السحابية الموزعة أن تقدم خدمات سحابية موجودة على مقربة أكبر بكثير من المستهلك ومن مصدر البيانات كذلك، وتتواصل مع خدمات سحابية أخرى لتقدم خدمات موزعة ومنخفضة الكمون وعالية الأداء.

وتشمل الحوسبة السحابية الموزعة توزيع أنواع قدرات الخدمات السحابية على حافة الشبكة لإتاحة تقديم خدمات سحابية منخفضة الكمون، تعالَج في الوقت الفعلي، على عرض نطاق محدود، بالعمل البيني مع مجموعة من الموارد المادية أو الافتراضية [ITU-T Y.3508]. ويجسد الشكل 6-1 أدناه مفاهيم الحوسبة السحابية الأساسية والحوسبة السحابية الإقليمية وحوسبة الحافة السحابية.



الشكل 6-1 مفهوم الحوسبة السحابية الموزعة

وللحوسبة السحابية الأساسية سِعة موردية كبيرة ومركز للإدارة الشاملة يتحكم في الموارد السحابية في الحوسبة السحابية الموزعة. وتدعم الحوسبة السحابية الأساسية الخدمات السحابية ذات الكثافة الحوسبية العالية، وغير المقيدة جغرافياً.

وتُنشر الحوسبة السحابية الإقليمية اختيارياً في أقاليم محددة حول موقع الحوسبة السحابية الأساسية بغرض تقاسم الحمولة معها وتحسين جودة الخدمة. وتتعامل الحوسبة السحابية الإقليمية مع طلبات الخدمات السحابية الواردة من الإقليم الذي تتحكم فيه الإدارة الشاملة للحوسبة السحابية الأساسية.

ملاحظة 1 – تدعم الحوسبة السحابية الإقليمية قيم كمون أدنى من تلك التي تدعمها الحوسبة السحابية الأساسية بتنفيذ خدمات سحابية مكيَّفة بحسب طلبات مستهلكي الخدمات السحابية (CSC) في الإقليم المعني. ويُفترض أن تكون قيمة كمون الشبكة من مستهلك الخدمة السحابية إلى الحوسبة السحابية الإقليمية أدنى من قيمة كمونها من مستهلك الخدمة السحابية إلى الحوسبة السحابية الأساسية، وأن تُنفَّذ الخدمات السحابية في الحوسبة السحابية الأساسية والإقليمية بفارق زمني لا يُذكر.

ملاحظة 2 – تؤدي الحوسبة السحابية الإقليمية وظيفتيْ التخزين المرحلي لحمولة الخدمة السحابية والتخزين المؤقت للبيانات الواردة من الحوسبة السحابية الأساسية، وتقدم هذه الخدمات والبيانات إلى مستهلك الخدمة السحابية في الإقليم المعني.

أما حوسبة الحافة السحابية، فتُنشر عند حافة الشبكة التي يَنفُذ إليها مستهلكو الخدمات السحابية وتُعرف بصغر سعتها الموردية. وتتطلب حوسبة الحافة السحابية موارد متخصصة من العتاد بحسب الغرض؛ أي أن موارد حوسبة الحافة السحابية محدودة، لأنها مقيَّدة بعاملي الحيز والقدرة. ويمكن أن تتضمن حوسبة الحافة السحابية تشكيلات متباينة لمواردها وأنواع شتى من قدرات الخدمات السحابية، ويتوقف نوع الموارد المادية والموارد الافتراضية على متطلبات مستهلكي الخدمات السحابية من هذه الخدمات وظروف بيئة النشر.

7 التحديات والتهديدات الأمنية المعرضة لها الحوسبة السحابية الموزعة

إن استخدام تكنولوجيا الحوسبة السحابية الموزعة يقدم مزايا من حيث السرعة العالية والكفاءة والأداء. لكنَّ استخدام الحوسبة السحابية الأساسية والحوسبة السحابية الإقليمية وحوسبة الحافة السحابية في الحوسبة السحابية الموزعة يطرح تحديات وتهديدات أمنية جديدة [ITU-T X.1601].

1.7 التحديات والتهديدات الأمنية المعرضة لها الحوسبة السحابية الأساسية

للحوسبة السحابية الموزعة بنى تحتية مختلفة الأحجام؛ فسعتها المورديةكبيرة في الحوسبة السحابية الأساسية أو الحوسبة السحابية الإقليمية، وصغيرة في حوسبة الحافة السحابية. وتستخدم الحوسبة السحابية الأساسية بنية تحتية غير متجانسةكنظام واحد يقدم خدمات مختلفة إلى مستهلكي الخدمات السحابية في الحوسبة السحابية الموزعة. وفيما يلي التحديات والتهديدات الأمنية التي يمكن أن تستهدف الحوسبة السحابية الأساسية:

(أ) **مواطن ضعف الأنظمة:** بالبنى التحتية للحوسبة السحابية الموزعة مواطن ضعف تتعلق بالأنظمة، خاصةً في الشبكات الحائزة لبنى تحتية معقدة ومنصات لأطراف ثالثة متعددة، ووجود موطن ضعف في الحوسبة السحابية الأساسية يؤثر أيضاً على الحوسبة السحابية الإقليمية وحوسبة الحافة السحابية.

(ب) **الأضرار المادية:** قد تُنشر البنى التحتية للحوسبة السحابية الموزعة في بيئات مادية غير موثوقة فتتضرر مادياً بفعل مستخدمين مخرِّبين أو سوء أحوال الطقس أو وقوع زلازل. وتَعرض الحوسبة السحابية الأساسية لأضرار مادية قد يؤثر كذلك على أمن الحوسبة السحابية الإقليمية وحوسبة الحافة السحابية.

2.7 التحديات والتهديدات الأمنية المعرضة لها الحوسبة السحابية الإقليمية

(أ) **اعتراض التناقل:** لا بد للحوسبة السحابية الأساسية من أن تتناقل البيانات مع الحوسبة السحابية الإقليمية، وقد تُعترض وصلات التناقل هذه.

(ب) **الأوامر أو الطلبات الزائفة:** إن ورود أمر أو طلب ضار من شبكة حوسبة سحابية أساسية أو حوسبة سحابية إقليمية أو حوسبة حافة سحابية مزيفة قد يسبب تسرب البيانات.

(ج) **مهاجمة السطوح البينية:** نظراً إلى أن ربط الحوسبة السحابية الأساسية بشبكات حوسبة سحابية إقليمية متعددة يتم عبر سطوح بينية مفتوحة، فقد تُهاجَم عبر هذه السطوح البينية.

(د) **هجمة الثقب الأسود:** يمكن لجهة دخيلة أن تخترق أحد الأجهزة أو تُدخل جهازاً مزيفاً إلى الشبكة ثم تستخدمه لشن ما يُدعى هجمة الثقب الأسود. وهجمة الثقب الأسود نوع من الهجمات التي تستهدف طبقة الشبكة يقوم فيها جهاز مخترَق بإرسال معلومات تسيير زائفة إلى الجهاز المجاور له ليجتذب حركة الشبكة إليه.

(هـ) **البوابات الاحتيالية:** من السهل على الجهة المهاجمة أن تنشر بوابة احتيالية. وبمجرد خداع أي من الأجهزة الشرعية ليتصل بالبوابة الاحتيالية، يمكن جمع معلومات التوصيل السرية. وهذا ما يسمح بالتحايل الفعال على العديد من التدابير الأمنية المنفذة وقد يسبب تداخلات راديوية للمُنشأة الرسمية للمنظمة.

(و) **النفاذ غير المخول لبوابات إنترنت الأشياء (IoT):** قد تَنفُذ الجهة المهاجمة إلى بوابات إنترنت الأشياء نفاذاً غير مخول، وهو ما قد يؤدي إلى كشف المعلومات الحساسة وتعديل البيانات والاستخدام غير المشروع لبعض موارد حوسبة الحافة السحابية.

3.7 التحديات والتهديدات الأمنية المعرضة لها حوسبة الحافة السحابية

(أ) **مشاكل تعدد الشاغلين:** لا تقدم العديد من حلول الخدمات السحابية الحماية الأمنية اللازمة فيما بين العملاء، الأمر الذي يؤدي إلى تقاسم الموارد والتطبيقات والأنظمة. وفي هذه الحالة، قد تنشأ تهديدات من عملاء آخرين داخل خدمة الحوسبة السحابية، وقد تؤثر التهديدات التي تستهدف عميل بعينه على عملاء آخرين كذلك.

(ب) **الطلبات الزائفة:** إذا اقترحت شبكة حوسبة سحابية إقليمية أو حوسبة حافة سحابية مزيفتان تنفيذ طلب ما، ولم تتعرف عليه شبكة الحوسبة السحابية الأساسية، فقد يؤدي ذلك إلى تسرب البيانات وما إلى ذلك.

(ج) **هجمة البرمجة النصية العابرة للمواقع (XSS):** قد تُشن هجمة برمجة نصية عابرة للمواقع لاستغلال مواطن الضعف القائمة في المواقع الإلكترونية بحقن شفرات ضارة في آلات العملاء، وانتحال إثباتات المستخدِمين لاستغلالها في مباشرة أنشطة ضارة.

(د) **الالتفاف على التوقيعات المحمية بلغة الوسم القابلة للتوسع (XML):** تشكل اللغة XML لغة الوسم الأساسية التي تُتيح استيقان منشأ التطبيقات في حوسبة الحافة السحابية. ويمكن للقراصنة أن يشنوا هجمات اختطاف لحسابات المستخدِمين باستعمال تقنية إعادة كتابة الرسائل المحمية باللغة XML أو تقنية الالتفاف على التوقيعات المحمية باللغة XML.

(هـ) **الإهمال من جانب الموظفين:** لا يزال الإهمال من جانب الموظفين مشكلةً من أكبر المشاكل الأمنية في جميع الأنظمة، لكنَّ التهديد الذي يمثله لإدارة الحوسبة السحابية الموزعة شديد الخطورة. إذ يمكن للموظفين الدخول إلى منصات إدارة الحوسبة السحابية الموزعة من هواتفهم المتنقلة أو أجهزتهم اللوحية المنزلية أو حواسيبهم الشخصية المنزلية، وقد يُعرِّضون بذلك النظام لتهديدات خارجية عديدة.

(و) **هجمات التصيُّد والهندسة الاجتماعية:** نظراً إلى انفتاح نظام الحوسبة السحابية الموزعة، فقد أصبحت هجمات التصيد والهندسة الاجتماعية شديدة الشيوع. فحال حصول المستخدم المخرِّب على معلومات تسجيل الدخول أو غيرها من المعلومات السرية، يمكنه اختراق النظام بسهولة.

(ز) **فقدان التحكم:** حينما تضع منظمة ما خدماتها على الحوسبة السحابية الموزعة، تفقد هذه الخدمات التحكم في الأماكن التي يمكن أن تخزَّن بها في الحيز السحابي، والقدرة على إدراكها. وفي الوقت نفسه، يصبح هذا الوضع مشكلةً أمنية من منظور المستخدِم لعدم درايته بالآليات الأمنية الممكنة لصوْن الخدمات التي يستخدمها.

(ح) **انتحال بيانات الأجهزة:** قد تتخفَّى الجهة المهاجمة في هيئة جهاز شرعي، ثم ترسل بيانات مزورة أو ضارة إلى حوسبة الحافة السحابية أو تسرق بيانات المستخدِمين.

(ط) **الاستيلاء على الأجهزة الطرفية:** توجد بالقرب من حوسبة الحافة السحابية أجهزة طرفية عديدة يمكنها جمع البيانات وإرسالها إلى حوسبة الحافة السحابية وتلقي النتائج أو الأوامر منها. ومن السهل اختراق الأجهزة الطرفية لضعف مستوى حمايتها الأمنية.

(ي) **هجمة رفض الخدمة الموزَّع (DDoS):** لقد زادت إلى حد كبير إمكانية تنفيذ هجمات رفض الخدمة الموزَّع. فإن شُرع في ضخ حركة ضارة إلى نظام الحوسبة السحابية بحجم كافٍ، قد ينهار نظام الحوسبة تماماً أو يتعرض لصعوبات. وبوجه خاص، تشكل حوسبة الحافة السحابية كياناً سحابياً صغيراً نسبياً بمستوى حماية أمنية ضعيف نسبياً، فمن الأرجح أن يستهدفها القراصنة بهجمات ويستخدمونها لتنفيذ هجمات لرفض الخدمة الموزَّع أو غير ذلك من الأنشطة غير القانونية.

(ك) **أمن التمثيل الافتراضي:** في بيئة حوسبة الحافة السحابية، يشمل ضمان أمن التمثيل الافتراضي تنفيذ تدابير للعزل والتعزيز الأمنيين لبوابات حوسبة الحافة السحابية ووحدات التحكم والمخدِّمات القائمة فيها، بتكنولوجيا التمثيل الافتراضي. ومقارنةً بالحوسبة السحابية الأساسية والحوسبة السحابية الإقليمية، تواجه عُقد حوسبة الحافة السحابية هذه، المحدودة الموارد التخزينية والموارد الحاسوبية، نواقل هجمات أعقد وأوسع انتشاراً.

8 مبادئ توجيهية أمنية لتكنولوجيا الحوسبة السحابية الموزعة

تقدم هذه الفقرة مبادئ توجيهية أمنية تتعلق بالحوسبة السحابية الأساسية والحوسبة السحابية الإقليمية وحوسبة الحافة السحابية في أنظمة الحوسبة السحابية الموزعة على النحو المبين في الفقرة 6.

1.8 مبادئ توجيهية أمنية للحوسبة السحابية الأساسية

تتضمن المبادئ التوجيهية الأمنية للحوسبة السحابية الأساسية مبادئ توجيهية بشأن أمن أنظمة الحوسبة السحابية الأساسية والأمن المادي والتدابير الأمنية لمكافحة رفض الخدمة وأمن الأجهزة الطرفية.

1.1.8 أمن أنظمة الحوسبة السحابية الأساسية

فيما يلي المبادئ التوجيهية لأمن أنظمة الحوسبة السحابية الأساسية:

(أ) يُوصى باستخدام أدوات للاستجابة للحوادث المدفوعة بمواطن ضعف الأنظمة.

(ب) يُوصى بمنع دخول البرمجيات الضارة إلى الخدمات السحابية بتقنيات من قبيل مسح الملفات، وإدراج التطبيقات في القائمة البيضاء، وكشف البرمجيات الضارة بتكنولوجيا تعلم الآلة، وتحليل حركة الشبكة.

(ج) يُوصى باستعراض تقييمات المخاطر وتحديثها لتشمل الخدمات السحابية. كما يُوصى بتحديد عوامل الخطر الناشئة عن بيئات الحوسبة السحابية الأساسية وتلك الناشئة بسبب مقدمي الخدمات، ومعالجتها. ويُتاح استخدام قواعد بيانات المخاطر المتعلقة بمقدمي الخدمات السحابية لتسريع عملية التقييم.

2.1.8 الأمن المادي

فيما يلي المبادئ التوجيهية للأمن المادي للحوسبة السحابية الأساسية:

(أ) يُوصى بإنشاء البنية التحتية للحوسبة السحابية الأساسية في موقع جغرافي مناسب، لا في مواقع من قبيل مسارات هبوط الطائرات ومحطات الكهرباء والسهول الفيضية وخطوط صدوع الزلازل أو غيرها من المناطق الشائع تعرضها لكوارث طبيعية.

(ب) يُوصى بتنفيذ عمليات تغيير وصيانة ورصد للظروف البيئية المادية للبنى التحتية المشيدة تحت الأرض.

(ج) يُوصى بتوفير أنظمة تبريد للبنى التحتية المشيدة تحت الأرض ووضع معايير امتثال تتعلق بهذه البنى التحتية.

(د) يُوصى بالحد من عدد المداخل في البنية التحتية للحوسبة السحابية الأساسية للحد من خطر الاختراقات.

(هـ) يُوصى بتزويد جميع أجزاء البنية التحتية للحوسبة السحابية الأساسية بنقاط تفتيش متعددة لتقليص خطر تمكُّن الجهات الدخيلة المخرِّبة من النفاذ إليها إلى أدنى درجاته.

(و) يُوصى بأن يوفر نظام الرصد والمراقبة مستوى إضافي من الأمن المادي.

(ز) يُوصى باستخدام خاصية التكرار في البنية التحتية للحوسبة السحابية الأساسية، لمساعدتها على تجاوز أي حوادث بأقصر فترة تعطل ممكنة.

3.1.8 مكافحة رفض الخدمة

فيما يلي المبادئ التوجيهية لمكافحة رفض الخدمة:

(أ) يُوصى بأن يكون مخدِّم الحوسبة السحابية الأساسية قادراً على التعامل مع طفرات ازدحام الحركة وأن يُزوَّد بأدوات التخفيف اللازمة لمعالجة المشاكل الأمنية.

(ب) يُوصى بتحديث وإصلاح جدران الحماية وبرامج أمن الشبكة بانتظام.

2.8 مبادئ توجيهية أمنية للحوسبة السحابية الإقليمية

تتألف المبادئ التوجيهية الأمنية للحوسبة السحابية الإقليمية من مبادئ توجيهية لأمن البيانات المتناقَلة والبيانات الثابتة وأمن السطح البيني المفتوح وأمن بوابات إنترنت الأشياء.

1.2.8 أمن البيانات المتناقَلة والبيانات الثابتة

تقدم الحوسبة السحابية الإقليمية خدمات الحوسبة السحابية الأساسية جزئياً أو كلياً في إقليم جغرافي معين. وتشمل المبادئ التوجيهية الأمنية المتعلقة بالبيانات المتناقَلة والبيانات الثابتة في الحوسبة السحابية الإقليمية ما يلي:

(أ) يُشترط أن تستخدم الحوسبة السحابية الإقليمية نظاماً للتجفير بقوة معينة لتجفير الاتصالات والبيانات. كما يُوصى بأن تدعم الحوسبة السحابية الإقليمية مأمونية خدمات بروتوكول النقل لمنع الهجمات القائمة على البروتوكول من المساس بالسرية.

(ب) يُشترط أن تستيْقن الحوسبة السحابية الإقليمية هويات الخدمات، وتُعرِّفها، وتُشدِّد استراتيجيات العزل الأمني ومراقبة النفاذ المقرر اعتمادها. ويُشترط أيضاً أن يُدعم تكييف استراتيجيات مراقبة النفاذ بحسب الطلب وإدارتها.

(ج) يُوصى بأن تدعم الحوسبة السحابية الإقليمية نظاماً للتبادل المأمون للبيانات، يرصد نسق البيانات ومحتواها وتدفقها وما شابه، ويتحكم فيه، في الوقت الفعلي.

(د) يُوصى بأن يستوفي نظام تبادل البيانات المأمون متطلبات مرنة عديدة في البيئة السحابية، منها تقديم أساليب نشر مرنة، وأساليب مرنة لجدولة الموارد، وأساليب للتبادل المأمون للبيانات على أساس العزل الأمني القوي للأعمال التجارية، وما إلى ذلك.

(هـ) يُوصى بأن تدعم الحوسبة السحابية الإقليمية كشف الشفرات الضارة وحذف البيانات المتناقَلة.

(و) يُشترط اعتماد آليات للتجفير والتحقق تضمن سلامة التخزين المحلي وسريته، بما في ذلك بيانات إدارة الأنظمة (كالملفات المفهرسة، ومعلومات ومفاتيح الخدمات السحابية)، ومعلومات الاستيقان، والبيانات التجارية المهمة (كبيانات خصوصية المستعمل).

(ز) يُوصى بأن يدعم نظام النفاذ إلى البيانات خاصية استيقان الهوية القائم على الأدوار، وباعتماد تدابير صارمة لمراقبة النفاذ لمكافحة النفاذ غير القانوني.

2.2.8 أمن السطح البيني المفتوح

من اللازم أن يوفر مقدم الخدمات السحابية (CSP) السطوح البينية للشبكات والسطوح البينية لبرمجة التطبيقات (API) التي تمكنه من تشكيل الخدمات السحابية المختلفة وإدارتها وتنسيقها ورصدها، وكذلك من تقديم الخدمات مباشرةً. وعادةً ما تنشأ أطراف ثالثة تقدم خدمات إضافية على أساس هذه السطوح البينية. وفيما يلي المبادئ التوجيهية لأمن السطوح البينية لبرمجة التطبيقات في الحوسبة السحابية الإقليمية:

(أ) يُشترط استخدام التجفير، كأسلوب أمن طبقة النقل (TLS) أو غيره من أساليب التجفير، في نقل الحالة التمثيلية (REST) للسطح API لتجفير البيانات أثناء تناقلها ومنع العبث بها. كما يُشترط استخدام آلية توقيع تضمن عدم إجازة فك تجفير البيانات وتعديلها إلا للمستخدمين الحائزين لحقوق النفاذ حصراً.

(ب) يُوصى بإنشاء هويات موثوقة للسطوح API عن طريق التأشيرات، ثم بعدم إجازة النفاذ إلى الخدمات وموارد البيانات وما إليها والتحكم فيها سوى للهويات الموثوقة التي تحمل التأشيرات فحسب.

(ج) يُوصى بإجراء عمليات رصد في الوقت الفعلي لسلوكيات استدعاء السطح البيني API المفتوح وحالات تناقل البيانات غير الاعتيادي كتقييد وتيرة النفاذ في السطح API، وبإصدار إنذارات بشأن هذه السلوكيات والحالات.

(د) يُوصى بالدأب على تبيُّن مواطن الضعف في السطوح API. ومن الممكن استخدام أدوات لكشف التسريبات الأمنية وتسرب البيانات في السطوح API، ولتتبُّع احتمالات تعرض هذه السطوح لهجمات وما قد يجري استغلاله من مواطن ضعف في الوقت الفعلي.

(هـ) يُوصى باستخدام البوابات الأمنية للسطوح API، كونها قد استُخدمت كتكنولوجيا أساسية لحماية أمن هذه السطوح. ونظراً إلى إمكانية استخدام البوابات الأمنية للسطوح API للتحكم في هذه السطوح وإدارتها، فيمكن لهذه البوابات أن تستيقنَ أيضاً مستخدمي كل من السطوح API وخدماتها.

3.2.8 أمن بوابات إنترنت الأشياء

تتصل أجهزة إنترنت الأشياء (IoT) بشبكة الإنترنت عبر بوابات إنترنت الأشياء، التي تصبح بالتالي الأهداف الرئيسية لهجمات البرمجيات الضارة والهجمات الشبكية. وفيما يلي المبادئ التوجيهية الأمنية لبوابات إنترنت الأشياء:

(أ) يُوصى بأن تدعم بوابات إنترنت الأشياء استيقان الأجهزة ومراقبة النفاذ إليها؛ فلا يُسمح بالنفاذ إلا للمستخدمين المخولين والأجهزة المصرح لها ولا يمكن لغيرهما تنفيذ عمليات تخزين أو خزائن مأمونة، حمايةً للمعلومات السرية كالمفاتيح والشهادات.

(ب) يُوصى بأن تدعم بوابات إنترنت الأشياء نظاماً لإدارة السياسات الأمنية يُعنى بتشكيل حقوق النفاذ والتحكم في نفاذ الأجهزة إلى خدمات التطبيقات (الخدمات التقنية والخدمات التجارية وخدمات البيانات) والملفات (ملفات التشكيل وملفات السِّجلات وملفات النُّسخ المتطابقة) وغيرها من الأشياء، وفقاً للسياسات الأمنية المعتمدة، وأن تكون البوابات قادرة على قطع التوصيلات والجلسات غير القانونية في الوقت المناسب.

(ج) يُوصى بأن تُتيح بوابات إنترنت الأشياء تنفيذ عمليات تحديث عبر الأثير (OTA) لضمان تشغيل البوابة لأحدث البرمجيات والبرمجيات الثابتة، تلافياً للشائع من مواطن الضعف والمخاطر. ومأمونية بدء التشغيل يمكن أن تضمن بدء تشغيل البوابة بنسخة برمجية ثابتة جرى التحقق من سلامتها واستيقانها، بما يمنع استخدام برمجيات ثابتة ضارة لبدء تشغيل البوابة.

(د) يُوصى بأن تدعم بوابات إنترنت الأشياء تنفيذ تدابير مختلفة للمراقبة الأمنية لحماية أجهزة إنترنت الأشياء. فعلى سبيل المثال، في حال استخدام بوابة إنترنت الأشياء كوسيط أمني في الشبكات والأجهزة، يُوصى بأن تُنفَّذ في البوابة جدران حماية، وعملية فرز للحركة بالاستناد إلى قواعد، ووظائف الإدراج في القائمة البيضاء.

(هـ) يُوصى بأن تدعم بوابات إنترنت الأشياء توفير سجلات تفصيلية للوقائع، لتمكين عمليات التدقيق الأمني من فهم العمليات المشغلة في البوابة، بعمق.

3.8 مبادئ توجيهية أمنية لحوسبة الحافة السحابية

تشتمل المبادئ التوجيهية الأمنية لحوسبة الحافة السحابية على مبادئ توجيهية لأمن البنية التحتية لحوسبة الحافة السحابية، وأمن شبكة حوسبة الحافة السحابية فيما يتعلق بالبيانات المتناقَلة والبيانات الثابتة وأمن الويب وأمن الأجهزة الطرفية المجاورة لحوسبة الحافة السحابية.

1.3.8 أمن البنية التحتية لحوسبة الحافة السحابية

تُوفر البنية التحتية لحوسبة الحافة السحابية الأساسيات البرمجية والعتادية، على السواء، ويشكل أمن هذه البنية التحتية متطلباً أساسياً من متطلبات حوسبة الحافة السحابية. وفيما يلي المبادئ التوجيهية الأمنية للبنية التحتية لحوسبة الحافة السحابية:

(أ) يُوصى بتوفير إطار خفيف للتمثيل الافتراضي لا يعتمد على العتاد وتنفيذ آليات للعزل والتعزيز الأمنيين.

(ب) يُوصى بتعزيز الحماية الأمنية للمشرف على الآلات الافتراضية ذاته والحد من نواقل الهجمات.

(ج) يُوصى بالتعاون مع مخدِّمات حوسبة الحافة السحابية، وبأن تتوفر في نظام التشغيل (OS) خاصيتا كشف الشفرات الضارة والوقاية منها، وعزل أمني قوي للتطبيقات، ودعم تهيئة بيئات تنفيذ موثوقة، وغيرها من الآليات الأساسية، لضمان سرية وسلامة مختلف التطبيقات المشغَّلة على نظام التشغيل، الذي يعاني من محدودية الموارد الحاسوبية أو الموارد التخزينية، بينما قد لا تتزامن السياسات والآليات الأمنية في الوقت المناسب مع الحوسبة السحابية الأساسية أو الحوسبة السحابية الإقليمية.

(د) يُوصى بأن يُنفِّذ مقدمو خدمات حوسبة الحافة السحابية عمليتي تعريف الهوية والاستيقان تنفيذاً تلقائياً وشفافاً وخفيف الوزن، ذلك أن عُقد حوسبة الحافة والبنية الديناميكية الشبكية للحوسبة السحابية الموزعة قد تؤديان إلى تكرار تعريف الهوية والاستيقان.

2.3.8 أمن شبكة حوسبة الحافة السحابية

نظراً إلى كثرة عدد عقد حوسبة الحافة السحابية وتعقيد طوبولوجيا شبكتها، الأمر الذي يزيد من مسارات الهجمات، فقد يسهل على الجهة المهاجمة أن ترسل إلى عقد حوسبة الحافة السحابية حِزَم بيانات شبكية ضارة، أو تشن هجمات رفض الخدمة، ليؤثر ذلك على اعتمادية شبكة حوسبة الحافة السحابية. وفيما يلي المبادئ التوجيهية الأمنية لشبكة حوسبة الحافة السحابية:

(أ) يُوصى بضمان أمن البروتوكول، في مرحلتي تصميمه وتنفيذه كلتيهما، الذي تستخدمه حوسبة الحافة السحابية لتلبية مختلف متطلبات مستهلكي الخدمات السحابية، المتعلقة بتناقل البيانات.

(ب) يُوصي بتعزيز البرتوكولات التي قد تكون عرضة للتأثر بالهجمات بسياسيات أمنية إضافية، بسبل منها تنفيذ عمليات تناقل البيانات عبر شبكة خاصة افتراضية (VPN) أو بأسلوب أمن طبقة النقل أو بغير ذلك من القنوات المأمونة بإضافة وحدات نمطية في البوابات.

(ج) يُوصى بإجراء عمليات تحقق من سلامة وأمن تناقل بيانات الشبكة فيما بين الآلات الافتراضية المنتمية إلى ميادين مختلفة، لضمان فعالية عزل مختلف وحدات الاتصالات التجارية. علاوةً على ذلك، يمكن لوحدات التحكم جدولة وحدات العزل النمطية في البيئة المتصوَّرة لتوفير قدرات العزل.

(د) يُوصى بإجراء عمليات رصد أمني لحركة الشبكة للإنذار بالحوادث الأمنية في الوقت المناسب، وتنفيذ أنشطة استجابة للحوادث بكفاءة. إضافةً إلى ذلك، يمكن لأنظمة الحماية أن تحجب الحركة الضارة مباشرةً.

3.3.8 أمن الويب في حوسبة الحافة السحابية

فيما يلي المبادئ التوجيهية لأمن الويب في حوسبة الحافة السحابية:

(أ) يُوصى بضمان فعالية رصد مرافق نظام حوسبة الحافة السحابية عن بُعد.

(ب) يُوصى بأن يقترن ضمان أمن حوسبة الحافة السحابية بجهود تثقيفية موسَّعة. فيُحاط الموظفون بما يمكنهم فعله بأجهزتهم وما لا يمكنهم فعله، ويتلقوْن المساعدة أيضاً للتعرف على المخاطر الأمنية.

(ج) يُوصى بضمان عدم وضع الأجهزة القديمة والبالية بجوار تلك الأكثر تعقيداً للحد من مواطن الضعف داخل الشبكة.

4.3.8 أمن الأجهزة الطرفية المجاورة لحوسبة الحافة السحابية

فيما يلي المبادئ التوجيهية لأمن الأجهزة الطرفية في حوسبة الحافة السحابية:

(أ) يُوصى بحجب النفاذ في حال محاولة جهاز شخصي غير مخول النفاذ إلى بيانات حوسبة الحافة السحابية.

(ب) يُوصى بأن تُشكَّل الحافة بقدرات تشمل خواصاً من قبيل الاستيقان القوي وتجفير عُقد الاستيقان.

(ج) يُوصى بأن تُدير البروتوكولات الأمنية لتكنولوجيا المعلومات (IT) ماهية الأجهزة التي يمكنها النفاذ إلى شبكة أنظمة حوسبة الحافة السحابية وأحوال ذلك.

(د) يُوصى بتهيئة بيئة حوسبة الحافة السحابية ورصدها باستمرار.

(هـ) يُوصى بأن يُفترض في الأجهزة الطرفية أنها مخترقة بالفعل، لا بالثقة تلقائياً في المعلومات الواردة منها؛ أي يُفترض أن جميع البيانات ضارة ما لم يثبت العكس.

(و) يُوصى بعدم إجازة التوصيل بالحوسبة السحابية الأساسية ونقل البيانات إليها إلا للأجهزة الطرفية المستيقَّنة.

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، 2023