الاتحـــــــــــاد الدولـــــــــــي للاتصـــــــــــالات

ITU-T

قطاع تقييس الاتصالات
في الاتحاد الدولي للاتصالات

X.1605

(2020/03)

السلسلة X: شبكات البيانات والاتصالات بين الأنظمة المفتوحة ومسائل الأمن

أمن الحوسبة السحابية – تصميم أمن الحوسبة السحابية

متطلبات أمن البنية التحتية كخدمة (IaaS) عمومية في الحوسبة السحابية

التوصية ITU-T X.1605

الاتحاد الدولي للاتصالات

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
الخصائص البيومترية	X.1080–X.1099
تطبيقات وخدمات آمنة (1)	
أمن البث المتعدد	X.1100–X.1109
أمن الشبكة المنزلية	X.1110–X.1119
أمن الخدمات المتنقلة	X.1120–X.1139
أمن الويب	X.1140–X.1149
بروتوكولات الأمن	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)	
الاتصالات في حالات 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.1360–X.1369
أمن أنظمة النقل الذكية (ITS)	X.1370–X.1389
أمن تكنولوجيا سجل الحسابات الموزع	X.1400–X.1429
أمن تكنولوجيا سجل الحسابات الموزع	X.1430–X.1449
بروتوكولات الأمن (2)	X.1450–X.1459
تبادل معلومات الأمن السيبراني	
نظرة عامة عن الأمن السيبراني	X.1500–X.1519
تبادل مواطن الضعف/الحالة	X.1520–X.1539
تبادل الأحداث/الأحداث العارضة/المعلومات الحدسية	X.1540–X.1549
تبادل 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
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
أشكال أخرى لأمن الحوسبة السحابية	X.1680–X.1699
الاتصالات الكمومية	X.1700–X.1729

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

التوصية ITU-T X.1605

متطلبات أمن البنية التحتية كخدمة (IaaS) عمومية في الحوسبة السحابية

ملخص

تواجه المنصات والخدمات الافتراضية في البنية التحتية كخدمة (IaaS) تحديات وتهديدات مختلفة، وربما أشد من تلك التي تواجهها البنية التحتية والتطبيقات التقليدية لتكنولوجيا المعلومات. وتحتاج منصات IaaS التي تتشارك في خدمات الحوسبة والتخزين والتوصيل الشبكي إلى حماية خاصة بالتهديدات في بيئة IaaS. وتهدف التوصية ITU-T X.1605 إلى توثيق متطلبات أمن البنية التحتية كخدمة عمومية من أجل مساعدة مقدمي IaaS على تحسين أمن منصة IaaS طوال مراحل التخطيط والبناء والتشغيل.

التسلسل التاريخي

الطبعة	التوصية	تاريخ الموافقة	لجنة الدراسات	معرف الهوية الفريد*
1.0	ITU-T X.1605	2020-03-26	17	11.1002/1000/14094

مصطلحات أساسية

الحوسبة السحابية، IaaS، متطلبات الأمن، الموارد الافتراضية.

* 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/.

© ITU 2020

جميع الحقوق محفوظة. لا يجوز استنساخ أي جزء من هذه المنشورة بأي وسيلة كانت إلا بإذن خطي مسبق من الاتحاد الدولي للاتصالات.

جدول المحتويات

الصفحة

1 مجال التطبيق 1
2 المراجع 1
3 التعاريف 1
1.3 مصطلحات معرفة في وثائق أخرى 1
2.3 مصطلحات معرفة في هذه التوصية 2
4 المختصرات والأسماء المختصرة 2
5 اصطلاحات 3
6 نظرة عامة 3
7 التحديات الأمنية في بيئة البنية التحتية كخدمة 5
8 متطلبات أمن طبقة النفاذ في البنية التحتية كخدمة 6
1.8 متطلبات أمن إلى شبكة الإنترنت 6
2.8 متطلبات أمن النفاذ إلى السطح البيني لبرمجة التطبيقات 6
9 متطلبات أمن طبقة خدمة IaaS 7
1.9 متطلبات أمن خدمة الحوسبة 7
2.9 متطلبات أمن خدمة التخزين 7
3.9 متطلبات أمن خدمة التوصيل الشبكي 8
10 متطلبات أمن طبقة موارد IaaS 8
1.10 متطلبات أمن كشف قدرات الموارد والتحكم فيها 8
2.10 متطلبات أمن المورد المادي 10
11 متطلبات إدارة الأمن 10
1.11 إدارة الهوية والتحكم في النفاذ 11
2.11 التدقيق الأمني 11
3.11 إدارة نقاط الضعف 12
4.11 الاستجابة للطوارئ 12
5.11 التعافي من الكوارث 12
6.11 النسخ الاحتياطي 13
بيبليوغرافيا 14

التوصية ITU-T X.1605

متطلبات أمن البنية التحتية كخدمة (IaaS) عمومية في الحوسبة السحابية

1 مجال التطبيق

تحلل هذه التوصية التحديات الأمنية التي يواجهها مقدمو البنية التحتية كخدمة (IaaS) في بيئة IaaS، وتحدد متطلبات أمن البنية التحتية كخدمة عمومية في الحوسبة السحابية. وتسري هذه التوصية على مقدمي البنية التحتية كخدمة.

وهذا وصف إجمالي لمتطلبات الأمن عند تنفيذ البنية التحتية كخدمة. أما إرشادات التنفيذ التفصيلية فهي خارج مجال تطبيق هذه الوثيقة.

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 إلى المراجعة، يرجى من جميع المستعملين لهذه التوصية السعي إلى 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.1642] التوصية ITU-T X.1642 (2016)، *مبادئ توجيهية من أجل الأمن التشغيلي للحوسبة السحابية.*

[ITU-T Y.3502] التوصية ITU-T Y.3502 (2014) | ISO/IEC 17789:2014، *تكنولوجيا المعلومات – الحوسبة السحابية – المعمارية المرجعية.*

[ITU-T Y.3513] التوصية ITU-T Y.3513 (2014)، *الحوسبة السحابية – المتطلبات الوظيفية للبنية التحتية كخدمة.*

[ISO/IEC 27002] ISO/IEC 27002:2013، *تكنولوجيا المعلومات – تقنيات الأمن – مدونة قواعد الممارسات المتعلقة بضوابط أمن المعلومات.*

[ISO/IEC 27031] ISO/IEC 27031:2011، *تكنولوجيا المعلومات – تقنيات الأمن – مبادئ توجيهية بشأن استعداد تكنولوجيا المعلومات والاتصالات لاستمرارية العمل.*

3 التعاريف

1.3 مصطلحات معرفة في وثائق أخرى

تستخدم هذه التوصية المصطلحات التالية المعرَّفة في وثائق أخرى:

1.1.3 الحوسبة السحابية (cloud computing) [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.

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

3.1.3 عميل الخدمة السحابية (cloud service customer) (CSC) [b-ITU-T Y.3500]: طرف يكون مرتبطاً بعلاقة تجارية لأغراض استخدام الخدمات السحابية.

4.1.3 شريك في الخدمة السحابية (cloud service partner) [b-ITU-T Y.3500]: طرف يشارك في دعم أنشطة إما مقدم الخدمة السحابية أو عميل الخدمة السحابية، أو يساعد في القيام بها.

5.1.3 مقدم الخدمة السحابية (cloud service provider) (CSP) [b-ITU-T Y.3500]: طرف يتيح توافر الخدمات السحابية.

6.1.3 البنية التحتية كخدمة (infrastructure as a service) (IaaS) [b-ITU-T Y.3500]: فئة من الخدمات السحابية تكون فيها القدرة المقدّمة لعميل الخدمة السحابية من نوع قدرات البنية التحتية.

7.1.3 تحدٍّ أمني (security challenge) [b-ITU-T X.1601]: "عقبة" أمنية مختلفة عن التهديدات الأمنية المباشرة، تنجم عن طبيعة الخدمات السحابية وبيئتها التشغيلية، بما في ذلك التهديدات "غير المباشرة".

8.1.3 نقطة ضعف (vulnerability) [b-NIST-SP-800-30]: مكمن ضعف في نظام المعلومات أو إجراءات أمن النظام أو أدوات الرقابة الداخلية أو التنفيذ يمكن استغلاله من قبل المصدر المهدِّد.

2.3 مصطلحات معرفة في هذه التوصية

لا توجد.

4 المختصرات والأسماء المختصرة

تستخدم هذه التوصية المختصرات والأسماء المختصرة التالية:

ACL	قائمة التحكم في النفاذ *(Access Control List)*
API	السطح البيني لبرمجة التطبيقات *(Application Programming Interface)*
BIA	تحليل التأثير التجاري *(Business Impact Analysis)*
CPU	وحدة المعالجة المركزية *(Central Processing Unit)*
CSC	عميل الخدمة السحابية *(Cloud Service Customer)*
CSP	مقدم الخدمة السحابية *(Cloud Service Provider)*
DDoS	الحرمان من الخدمة الموزَّع *(Distributed Denial of Service)*
DSP	مقدم الخدمة السحابية *(Digital Service Provider)*
IAM	إدارة خدمات الهوية والنفاذ *(Identity and Access Management)*
IaaS	البنية التحتية كخدمة *(Infrastructure as a Service)*
ICT	تكنولوجيا المعلومات والاتصالات *(Information and Communication Technology)*
IdM	إدارة الهوية *(Identity Management)*
I/O	دخل/خرج *(Input/Output)*
NIC	بطاقة السطح البيني للشبكة *(Network Interface Card)*
OS	نظام التشغيل *(Operating System)*
OTT	الخدمات المتاحة بحرية على الإنترنت *(Over The Top)*
PaaS	المنصات كخدمة *(Platform as a Service)*

RPO هدف نقطة الاستعادة *(Recovery Point Objective)*

RTO أهداف وقت الاستعادة *(Recovery Time Objectives)*

SaaS البرمجيات كخدمة *(Software as a Service)*

SLA اتفاق مستوى الخدمة *(Service Level Agreement)*

SQL لغة الاستعلام البنيوية *(Structured Query Language)*

VDC مركز البيانات الافتراضية *(Virtual Data Centre)*

VLAN شبكة محلية افتراضية *(Virtual Local Area Network)*

VM آلة افتراضية *(Virtual Machine)*

VXLAN شبكة محلية افتراضية قابلة للتوسعة *(Virtual Extensible Local Area Network)*

XSS الشفرة المندسة عبر مواقع إلكترونية *(Cross Site Script)*

5 اصطلاحات

في هذه التوصية، تشير كلمة "يُتطلب/يتعيَّن/يلزم/يجب" إلى متطلَّب يجب التقيد به على نحو صارم ولا يجوز أي حيدان عنه إذا أريد إعلان المطابقة مع مقتضيات هذه التوصية.

وتشير كلمة "يُوصَى" إلى متطلَّب يُوصى به لكنه ليس ملزِماً إلزاماً مطلَقاً. وبالتالي لا يستلزم إعلانُ المطابقة تحقُّقَ هذا المتطلَّب.

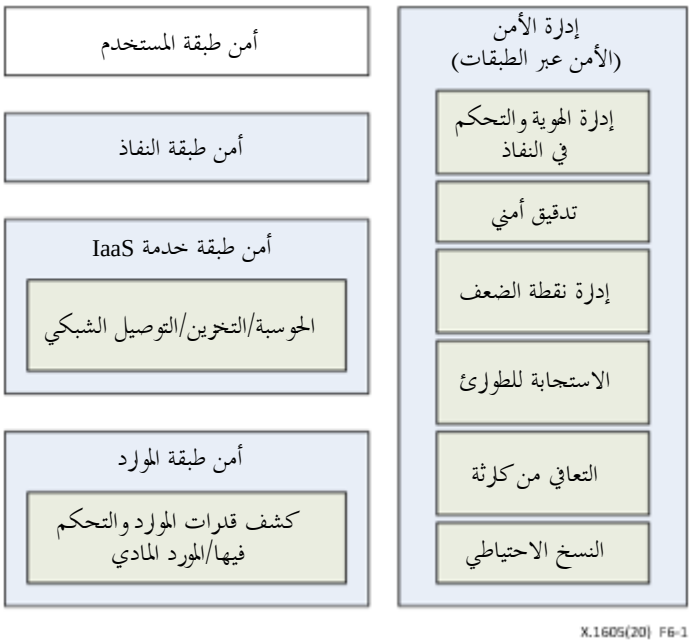
وتشير عبارة "يتاح خيار/يكون من المتاح خيار"، إلى متطلَّب اختياري جائز، ولا تنطوي على أي إيحاء بالتوصية به. ولا يُرمى من هذه العبارة إلى الإيحاء بأن قيام الجهة البائعة بالتنفيذ يجب أن يشتمل على توفير الوظيفة المعنية بمثابة خيار بحيث يتاح لمشغِّل الشبكة/موفِّر الخدمة إعمالها اختيارياً. بل إنها تعني أنه يجوز للجهة البائعة أن تختار توفير هذه الوظيفة أو عدم توفيرها دون أن يؤثر ذلك على إعلانها مطابقة المواصفة المعنية.

وفي متن هذه التوصية وملحقاتها، تظهر في بعض الأحيان كلمات يتعين، ويتعين ألا، وينبغي، ويمكن. وفي هذه الحالة يكون تأويلها، على التوالي، على "يجب"، أو "يلزم"، أو "مطلوب"، و"يجب ألا"، أو "يلزم ألا"، أو "يحظر"، و"يوصي"، و"يجوز اختيارياً"، أو "من الجائز اختيارياً". ويأوّل انتفاء القصد المعياري عند ظهور مثل هذه العبارات أو الكلمات الرئيسية في تذييل أو في مادة موسومة صراحةً على أنها إعلامية.

6 نظرة عامة

البنية التحتية كخدمة هي فئة من الخدمات السحابية، حيث يكون نوع القدرات السحابية المقدمة إلى عميل الخدمة السحابية (CSC) نوعاً من قدرات البنية التحتية [b-ITU-T Y.3500]. وتتيح IaaS لعملاء الخدمة السحابية استخدام موارد البنية التحتية السحابية (الحوسبة أو التخزين أو التوصيل الشبكي) التي يمكن تقديمها وإصدارها بسرعة بالحد الأدنى من جهود الإدارة. وتمكّن خدمات البنية التحتية كخدمة عمومية عملاء الخدمة السحابية من إطلاق أعمالهم بسرعة وسهولة دون إنشاء بنية تحتية جديدة لتكنولوجيا المعلومات والاتصالات (ICT)، ويمكن لعملاء الخدمة السحابية استخدام هذه الموارد لتطوير واستضافة وتشغيل الخدمات والتطبيقات عند الطلب بطريقة مرنة حسب الحاجة.

واستناداً إلى إطار الطبقات الذي تم تطويره مع المنظمة الدولية للتوحيد القياسي (ISO)/اللجنة الكهرتقنية الدولية (IEC) على النحو المعرَّف في التوصية [ITU-T Y.3502] والمفهوم الإجمالي للبنية التحتية كخدمة المعرَّف في التوصية [ITU-T Y.3513]، ويوضح الشكل 6-1 المفهوم الإجمالي لمتطلبات أمن البنية التحتية كخدمة.



الشكل 6-1 المفهوم الإجمالي لمتطلبات أمن البنية التحتية كخدمة

طبقة المستخدم هي السطح البيني للمستخدم الذي يتفاعل عبره عميل الخدمة السحابية مع مقدم الخدمة السحابية (CSP). وتشمل المكونات الوظيفية لطبقة المستخدم وظيفة المستخدم ووظيفة الأعمال ووظيفة الإداري، وهي تتفاعل مع الخدمات السحابية التي يقدمها مقدم الخدمة السحابية، وتؤدي الأنشطة الإدارية المتعلقة بعميل الخدمة السحابية ومراقبة الخدمات السحابية. ووفقاً للمسؤوليات بين مقدم الخدمة السحابية وعميل الخدمة السحابية، ينبغي أن يتولى عملاء الخدمة السحابية قيادة آليات الأمن بطبقة المستخدم لأنهم يستخدمون عادة أدواتهم أو أنظمة هم الخاصة للنفاذ إلى خدمة IaaS. وإذا كان الأمر خلاف ذلك، يقدم مقدم الخدمة السحابية أدوات أو أنظمة طبقة المستخدم، وينبغي أن يقدم مقدم الخدمة السحابية الأدوات أو الأنظمة التي تلبي أفضل ممارسات الصناعة للأمن. وتقع متطلبات أمن طبقة المستخدم خارج مجال تطبيق هذه التوصية.

وتقدم طبقة النفاذ سطحاً بينياً مشتركاً للنفاذ اليدوي والمؤتمت معاً إلى القدرات المتاحة في طبقة الخدمة. وتشمل المكونات الوظيفية لطبقة النفاذ التحكم في النفاذ وإدارة التوصيل. وتتولى طبقة النفاذ مسؤولية تقديم قدرات خدمة IaaS عبر آلية نفاذ واحدة أو أكثر مثل السطوح البينية لمواقع الويب ولبرمجة التطبيقات (API). ويرد تعريف متطلبات أمن طبقة النفاذ في الفقرة 8.

وتحتوي طبقة الخدمة على تنفيذ خدمات IaaS التي يقدمها مقدم الخدمة السحابية. فهي تحتوي على المكونات البرمجية التي تنفذ خدمات IaaS وتتحكم فيها، وترتب تقديم الخدمات إلى عميل الخدمة السحابية عبر طبقة النفاذ. ويرد تعريف متطلبات أمن طبقة الخدمة في الفقرة 9.

وتشمل مكونات طبقة الموارد كشف قدرات الموارد والتحكم فيها، والموارد المادية على النحو المعرَّف في التوصية [ITU-T Y.3502]. وتتولد الموارد الافتراضية ويُتحكم فيها من خلال كشف قدرات البرمجيات. ويرد تعريف متطلبات أمن طبقة الموارد في الفقرة 10.

وتقدم إدارة الأمن قدرات أساسية لإدارة الأمن عبر الطبقات، والتي تنفَّذ عبر طبقة المستخدم وطبقة النفاذ وطبقة الخدمة وطبقة الموارد على النحو الموضح أعلاه. ويرد تعريف متطلبات إدارة الأمن لإدارة الهوية والتحكم في النفاذ، والتدقيق الأمني، وإدارة نقاط الضعف، والاستجابة للطوارئ، والتعافي من الكوارث، والنسخ الاحتياطي في الفقرة 11.

7 التحديات الأمنية في بيئة البنية التحتية كخدمة

نظراً للمزايا الهائلة لنظام البنية التحتية كخدمة، أصبحت البنية التحتية كخدمة إحدى أهم خدمات مقدمي الخدمة السحابية خاصة لمشغلي الاتصالات التقليديين ومقدمي الخدمات المتاحة بحرية على الإنترنت (OTT) ومقدمي الخدمات الرقمية (DSP) فتوسعت توسعاً سريعاً. وبموازاة تطور IaaS السريع، تظل المشكلات الأمنية مصدر قلق كبير وهام لا يمكن تجاهله. والتحديات والتهديدات التي تتعرض لها منصات وخدمات IaaS تفوق تلك التي تتعرض لها البنية التحتية والتطبيقات التقليدية لتكنولوجيا المعلومات، خاصةً بسبب التنفيذ الواسع لتقنيات المحاكاة الافتراضية والموارد المشتركة لمستأجرين متعددين في جملة أسباب أخرى.

ونظراً لأن البنية التحتية كخدمة عمومية يمكن أن تخدِّم العديد من عملاء الخدمة السحابية من العديد من المؤسسات المختلفة التي تتعايش مع بعضها البعض، فإن الأمن وحماية الخصوصيات على السواء هما أهم العوامل عندما يقيِّم عملاء الخدمة السحابية اختيار خدمات البنية التحتية كخدمة عمومية.

وباختصار، يمكن أن تظهر التحديات الأمنية التي تواجهها البنية التحتية كخدمة عمومية من الجوانب التالية:

1) المحاكاة الافتراضية: كميزة تقنية مهمة للحوسبة السحابية، تمكّن تقنية المحاكاة الافتراضية مختلف الآلات الافتراضية (VM) المشغَّلة على المشرف نفسه ولكنها تجعل أيضاً الملفات التي تتضمنها الآلات الافتراضية عرضة للتعديل بشكل غير قانوني. وعلاوةً على ذلك، بمجرد استغلال نقاط ضعف المشرف على الآلات الافتراضية، ستواجه جميع الآلات الافتراضية المشغَّلة عليه نفس المخاطر الأمنية. ويمكن أن تنجم هذه المخاطر عما يلي:
   - التشكيلة غير المناسبة وعزل الشبكة للمضيفين الماديين. ويمكن للمهاجمين الاستفادة بشكل مباشر من نقاط الضعف في المشرف على الآلات الافتراضية.
   - نقاط الضعف في سطوح التماس بين الآلات الافتراضية والمشرف عليها. ويمكن أن يستغل المهاجمون الثغرات الأمنية للتحكم في المشرف على الآلات الافتراضية، الأمر الذي يسمى فرار الآلة الافتراضية.
2) السطوح البينية المفتوحة لبرمجة التطبيقات: كمنطلق لإدارة الآلات الافتراضية تلقائياً، يمكن للسطوح البينية المفتوحة لبرمجة التطبيقات أن توسع سطح الهجوم من خلال استغلال نقاط ضعف أو العبث بها ومثال نقاط الضعف هذه الافتقار إلى الاستيقان أو التخويل أو التحقق من السلامة، ومن شأن ذلك أن يدمر العديد من التطبيقات.
3) توصيلية الشبكة والإنترنت: لا تُطلَق تهديدات الشبكة مثل هجمات الحرمان من الخدمة الموزَّع (DDoS)، وهجوم من طرف متوسط بين طرفين، وهجوم انتحال بروتوكول الإنترنت، وما إلى ذلك، من الشبكة التقليدية فحسب، بل يمكن أن تُشن أيضاً من آلات افتراضية في نفس الآلة المضيفة وهو ما يجعل الدفاع أصعب بكثير داخل بيئة الحدود المبهمة لشبكة المحاكاة الافتراضية.
4) درجة عالية من التشارك في الموارد: يمكن أن تقدم هذه الصفة التقنية هدفاً أكثر تحديداً. وفي حال تدمير الآلة المضيفة المادية أو الشبكة المادية، ستتأثر جميع آلاتها الافتراضية. ويتعلق التخلص من أجهزة التخزين المسحوبة من التداول أو أجهزة التخزين المبدَّلة بسرية بيانات جميع عملاء الخدمة السحابية. وهو أيضاً سيصعِّب العزل بين مختلف عملاء الخدمة السحابية. وإذ لم يشكَّل عزل مختلف الأجهزة الافتراضية بشكل صحيح، فقد تزداد كثيراً إمكانية تسرب البيانات أو حتى هجمات الشبكة بين الآلات الافتراضية المختلفة. وستؤدي أي حوادث تقع إلى مخاطر وعواقب أمنية كبيرة.
5) قابلية التوسع التناسبي في الموارد الافتراضية: يؤدي التوسع المرن للموارد الافتراضية والتعديل الدينامي للمحيط الأمني للشبكة الافتراضية إلى نمو سريع في تدفق الحركة من مخدِّم إلى آخر في الشبكة ومطالب أمنية جديدة معقدة. ويتطلب ذلك خفة حركة المرافق الأمنية وقدرتها على العمل التعاوني، لكن معظم المعدات والأنظمة الأمنية تعمل بشكل فردي وتفتقر إلى آلية التعاون الفعال.
6) إدارة التشكيلة: تحتوي بيئة الحوسبة السحابية على أنواع مختلفة وكمية هائلة من الأصول، وأنواع مختلفة من الخدمات، مما يؤدي إلى كثرة الطلبات من التشكيلة بما في ذلك التحكم في النفاذ والعزل والنسخ الاحتياطي للبيانات وما إلى ذلك. وقد تكشف التشكيلة غير الصحيحة سطح هجوم جديد، أو حتى تسرب معلومات حساسة مباشرة.

7) قضايا التسجيل: يمكن لبيانات السجلات المختلفة في أنظمة التشغيل والتطبيقات ومعدات الأمن أن تساعد المشغلين على تجنب الكوارث مقدماً، وحتى اكتشاف السبب الجذري للحوادث الأمنية. وفي بيئة الحوسبة السحابية، أصبح الحصول على السجل وحمايته ومزامنة الوقت أكثر تعقيداً. فعلى سبيل المثال، من شأن إغفال حماية السجل أن يعرضه لخطر التلاعب، في حين أن الافتقار إلى مزامنة الوقت يصعِّب تلازم السجلات غير المتجانسة.

8 متطلبات أمن طبقة النفاذ في البنية التحتية كخدمة

تتولى طبقة النفاذ في البنية التحتية كخدمة مسؤولية عرض قدرات خدمة IaaS على عملاء الخدمة السحابية للنفاذ إلى آلية نفاذ واحدة أو أكثر وإدارتها. وتتضمن آليات النفاذ على سبيل المثال لا الحصر ما يلي:

- النفاذ إلى شبكة الإنترنت.
- النفاذ إلى السطح البيني لبرمجة التطبيقات.

وتتمثل المسؤولية الأخرى لطبقة النفاذ في تنفيذ آليات إدارة التوصيل المناسبة لتقديم إنفاذ سياسات جودة الخدمة، وتوازن الحمولة والإرسال الآمن فيما يتعلق بالحركة والتوصيلات من و/أو إلى المكونات الوظيفية لطبقة المستخدم.

1.8 متطلبات أمن إلى شبكة الإنترنت

1) يُتطلب من مقدم الخدمة السحابية IaaS تطبيق تدابير الاستيقان والتخويل على عميل الخدمة السحابية للنفاذ إلى خدمة IaaS من خلال النفاذ إلى شبكة الإنترنت، من قبيل الاستيقان من الطلب من خلال بيانات اعتماد عميل الخدمة السحابية والتحقق من صحة تخويل عميل الخدمة السحابية.

2) يُتطلب من مقدم الخدمة السحابية IaaS تطبيق آلية التحكم في النفاذ كي يستخدم عميل الخدمة السحابية قدرات الخدمة ذات الصلة.

3) يوصى بأن يقدم مقدم الخدمة السحابية IaaS نفق اتصالات آمناً لعميل الخدمة السحابية من خلال النفاذ إلى شبكة الإنترنت.

4) يوصى بأن يقدم مقدم الخدمة السحابية IaaS إلى عميل الخدمة السحابية حماية النفاذ إلى شبكة الإنترنت، من قبيل التحقق من صحة المدخلات والمخرجات، والتحقق من سلامة الطلب، والقدرات الدفاعية ضد سلوكيات التسلل في شبكة الإنترنت، مثل حقن لغة الاستعلام البنيوية (SQL)، والشفرة المندسة عبر مواقع إلكترونية (XSS)، تنفيذ الأوامر عن بُعد، وما إلى ذلك.

5) يُتطلب من مقدم الخدمة السحابية IaaS دعم قدرات محصنة ضد التلاعب للقيام بتسجيل الدخول والتحليل والتدقيق الأمني لسلوكيات النفاذ إلى شبكة الإنترنت.

2.8 متطلبات أمن النفاذ إلى السطح البيني لبرمجة التطبيقات

1) يُتطلب من مقدم الخدمة السحابية IaaS دعم الاستيقان واستيقان بيانات اعتماد المستخدم لدى عميل الخدمة السحابية عند استدعاء السطح البيني لبرمجة تطبيقات الخدمة، من قبيل تسجيل الدخول إلى السطح البيني لبرمجة التطبيقات لضمان استخدام المتصلين المشروعين حصراً.

2) يُتطلب من مقدم الخدمة السحابية IaaS تقديم آلية التحكم في النفاذ لعميل الخدمة السحابية عند استدعاء السطح البيني لبرمجة تطبيقات الخدمة.

3) يوصى بأن يقدم مقدم الخدمة السحابية IaaS نفق اتصالات آمناً لعميل الخدمة السحابية من خلال النفاذ إلى السطح البيني لبرمجة التطبيقات.

4) يوصى بأن يقدم مقدم الخدمة السحابية IaaS إلى عميل الخدمة السحابية حماية السطح البيني لبرمجة التطبيقات، من قبيل التحقق من سلامة الطلب، والقدرات الدفاعية ضد سلوكيات الهجوم، مثل هجوم الإعادة، وحقن الشفرة، وما إلى ذلك.

5) يُتطلب من مقدم الخدمة السحابية IaaS دعم قدرات تسجيل الدخول والتحليل والأمن لسلوك استدعاء السطح البيني لبرمجة التطبيقات.

9 متطلبات أمن طبقة خدمة IaaS

تحتوي طبقة الخدمة الخاصة بالبنية التحتية كخدمة على تنفيذ الخدمات التي يقدمها مقدم الخدمة السحابية. وتحتوي طبقة الخدمة على مكونات البرمجيات التي تنفذ خدمات IaaS (مثل خدمة الحوسبة وخدمة التوصيل الشبكي وخدمة التخزين وما إلى ذلك) وتتحكم فيها، وترتب تقديم خدمات IaaS هذه إلى عملاء الخدمة السحابية عبر طبقة النفاذ.

1.9 متطلبات أمن خدمة الحوسبة

1) يُتطلب من مقدم الخدمة السحابية IaaS تقديم آليات عزل للموارد الافتراضية، بما في ذلك عزل وحدة المعالجة المركزية (CPU) والشبكة الداخلية والذاكرة والتخزين، وما إلى ذلك، والسماح حصراً بالاتصالات الملتزمة بسياسة الأمن بين وحدات الموارد الافتراضية المختلفة، مثل الآلات الافتراضية.

2) يُتطلب من مقدم الخدمة السحابية IaaS دعم إعداد الحد الأعلى للمورد من أجل وحدة مورد افتراضية واحدة في مضيف مادي، مما من شأنه تجنب تردي الأداء الناجم عن الإشغال المفرط لوحدة مورد افتراضية محددة.

3) يوصى بأن يدعم مقدم الخدمة السحابية IaaS الانتقال التلقائي لوحدة مورد افتراضية في حال تعطل المخدِّم المستضاف، مما من شأنه منع انقطاع الخدمات المشغَّلة في المورد الافتراضي.

4) يُتطلب من مقدم الخدمة السحابية IaaS دعم التحقق من سلامة ملفات صور وحدات موارد افتراضية لمنع التلاعب الخبيث، وضمان حصر تثبيت وحدة تخزين منطقية بوحدة مورد افتراضية واحدة في وقت واحد.

5) يُتطلب من مقدم الخدمة السحابية IaaS دعم انتقال سياسة الأمن الذي سيتم مزامنته في نفس الوقت مع وحدة المورد الافتراضية تبعاً لذلك.

6) يُتطلب من مقدم الخدمة السحابية IaaS تزويد إداري عميل الخدمة السحابية بالقدرة على تفصيل سياسة الأمن على المقاس بين وحدات الموارد الافتراضية.

7) يُتطلب من مقدم الخدمة السحابية IaaS تزويد عميل الخدمة السحابية بالقدرة على الحذف الكامل لبياناته. فبمجرد إزالة عميل الخدمة السحابية لوحدة مورد افتراضية، ينبغي أيضاً حذف ملفات الصور واللقطات والنسخ الاحتياطية في وقت واحد.

2.9 متطلبات أمن خدمة التخزين

1) يوصى بأن يدعم مقدم الخدمة السحابية IaaS آلية تكرار البيانات الرديف. وينبغي ضمان بيانات عملاء الخدمة السحابية بما لا يقل عن نسختين احتياطيتين في مواقع مادية مختلفة، وينبغي أن تكون الآلية شفافة بالنسبة إلى عملاء الخدمة السحابية.

2) يوصى بأن يدعم مقدم الخدمة السحابية IaaS التحكم المتزامن في الدخل/الخرج (I/O) والنفاذ المتوازي الآمن لعدة آلات افتراضية باستخدام نظام التخزين نفسه.

3) يُتطلب من مقدم الخدمة السحابية IaaS ضمان التحكم في النفاذ إلى البيانات المخزنة التي يمكن تنفيذها على كيانات التخزين المنطقي والمادي التي ينبغي عدم تجاوزها بأي تغيير في الموقع الفعلي للتخزين.

4) يُتطلب من مقدم الخدمة السحابية IaaS ضمان إمكانية حذف بيانات عملاء الخدمة السحابية بالكامل بما في ذلك:

- ينبغي القيام بحذف البيانات بالكامل قبل إعادة تخصيص مورد التخزين إلى عميل خدمة سحابية جديد.
- بمجرد حذف ملفات/كائنات عميل الخدمة السحابية، تنبغي على النحو المناسب الكتابة فوق وحدة التخزين المادية المقابلة أو وسمها على أنها للكتابة حصراً، وتجنب الاسترداد غير المجاز
- بمجرد انتقال بيانات عميل الخدمة السحابية، يُتطلب حذف البيانات الشرحية لعميل الخدمة السحابية تماماً وفوراً.

3.9 متطلبات أمن خدمة التوصيل الشبكي

1) يوصى بأن يزود مقدم الخدمة السحابية IaaS عميل الخدمة السحابية بالقدرة على مراقبة حركة موارده الافتراضية ضمن الشبكة من عميل إلى مخدِّم ومن مخدِّم إلى آخر

2) يوصى بأن يزود مقدم الخدمة السحابية IaaS عميل الخدمة السحابية بالقدرة على تنفيذ التحكم في عرض نطاق الموارد الافتراضية في السطح البيني للشبكة.

3) يُتطلب من مقدم الخدمة السحابية IaaS تقديم تدابير عزل بين الشبكة الافتراضية لعملاء الخدمة السحابية ومنصة IaaS وشبكة الإدارة، مثل منع عميل الخدمة السحابية من النفاذ إلى الآلة المضيفة أو عقدة الإدارة.

4) يُتطلب من مقدم الخدمة السحابية IaaS تنفيذ آلية قائمة التحكم في النفاذ إلى الشبكة (ACL) لتحقيق العزل الأمني والتحكم في النفاذ ضمن الشبكات الافتراضية.

5) يوصى بأن يدعم يزود مقدم الخدمة السحابية IaaS الدفاع ضد هجمات على الشبكة مثل القفز إلى شبكة محلية افتراضية (VLAN) أو إلى شبكة محلية افتراضية قابلة للتوسعة (VXLAN).

10 متطلبات أمن طبقة موارد IaaS

وفقاً للمكونات الوظيفية لطبقة موارد IaaS، تشمل متطلبات أمن طبقة موارد IaaS ما يلي:

- متطلبات أمن كشف قدرات الموارد والتحكم فيها؛
- متطلبات أمن الموارد المادية.

1.10 متطلبات أمن كشف قدرات الموارد والتحكم فيها

إن المكون الوظيفي لكشف قدرات الموارد والتحكم فيها يمكِّن مقدمي الخدمة السحابية من عرض ميزات مثل المرونة السريعة وتجميع الموارد والخدمة الذاتية عند الطلب. وهو يتضمن تجميع الموارد الافتراضية (مثل، مورد الحوسبة الافتراضية، ومورد الشبكة الافتراضية، وما إلى ذلك)، ومنصة إدارة الموارد الافتراضية. وستتوضح متطلبات أمن كشف قدرات الموارد والتحكم فيها من منظور تقديم الموارد الافتراضية وإدارتها.

1.1.10 متطلبات أمن تجميع الموارد الافتراضية

1.1.1.10 متطلبات أمن مورد الحوسبة الافتراضي

1) يُتطلب عزل وحدات موارد الحوسبة الافتراضية (مثل الآلة الافتراضية، والحاوية، وما إلى ذلك) منطقياً عن بعضها البعض.

2) يُتطلب ألا تتأثر وحدة موارد الحوسبة الافتراضية بوحدات أخرى أو آلات مضيفة عندما تصادف حوادث أو أعطال غير طبيعية.

3) يُتطلب ألا تستخدم وحدة موارد الحوسبة الافتراضية بما يزيد عن حصتها.

4) يوصى بحظر "النسخ" و"اللصق" وغيرها من الأوامر بين وحدات موارد الحوسبة الافتراضية المختلفة أو الآلات المضيفة.

5) يوصى بأن يدعم مقدم الخدمة السحابية IaaS مراقبة الموارد الافتراضية في الوقت الفعلي بأسلوب ضمن النطاق أو خارج النطاق، وإرسال إنذارات بمجرد اكتشاف حالات شاذة. وبالنسبة لكل وحدة موارد افتراضية، ينبغي أن تتضمن الكائنات المراقَبة حالة التشغيل، وحالة استهلاك الموارد والانتقال، وما إلى ذلك.

2.1.1.10 متطلبات أمن موارد الشبكة الافتراضية

1) يُتطلب عزل الشبكة الافتراضية لعميل الخدمة السحابية منطقياً عن بعضها البعض من خلال تنفيذ تدابير VLAN وVXLAN وACL وما إلى ذلك.

2) يُتطلب تقديم قدرة مراقبة حركة الشبكة بين وحدات الموارد الافتراضية المختلفة.

3) يُتطلب تقديم قدرة التحكم في مدل البتات عبر المنافذ الافتراضية.

4) يوصى بكشف سلوكيات الهجوم على الشبكة (مثل انتحال بروتوكول الإنترنت (IP) والديدان البرمجية وما إلى ذلك)، الصادرة من داخل الموارد الافتراضية، ومنعها.

5) يُتطلب حظر الأسلوب المتسيب لمنافذ بطاقة السطح البيني للشبكة (NIC) الافتراضية لمنع التجسس على حركة الشبكة.

3.1.1.10 متطلبات أمن موارد التخزين الافتراضية

1) يُتطلب عزل تجمع موارد التخزين الافتراضية بين مختلف عملاء الخدمة السحابية.

2) يُتطلب تنفيذ تدابير الأمن على البيانات المخزنة في كيانات التخزين المنطقية والمادية.

3) يُتطلب حظر النفاذ المباشر إلى موارد التخزين المادية.

4) تُتطلب القدرة على التحكم المتزامن في الدخل/الخرج والنفاذ المتوازي الآمن لدعم وحدات موارد افتراضية متعددة تستخدم كيانات التخزين نفسها.

5) يوصى بأن تدعم موارد التخزين الافتراضية التوسع المرن دون تعطيل خدمات التخزين العادية.

1.2.10 متطلبات أمن منصة إدارة الموارد الافتراضية

1) يُتطلب تنفيذ تدابير التحكم في النفاذ بشكلٍ مناسب لمنع النفاذ غير القانوني إلى منصة إدارة الموارد الافتراضية.

2) يوصى الاكتفاء بتثبيت المكونات والتطبيقات الضرورية وإغلاق منافذ الخدمة غير ذات الصلة، عملاً بمبدأ تقليل المخاطر إلى أدنى حد.

3) يُتطلب اكتشاف السلوكيات المهاجمة على منصة إدارة الموارد والإنذار بشأنها في الوقت المناسب، وينبغي تدوين السجلات بما في ذلك عنوان بروتوكول الإنترنت للمصدر ونوع الهجوم والختم الزمني وما إلى ذلك.

4) يُتطلب تقديم قدرة المراقبة في الوقت الفعلي على الموارد الافتراضية بما في ذلك حالة التشغيل، وإشغال المورد، والانتقال، وما إلى ذلك.

5) يوصى بتعطيل الموارد الافتراضية غير الضرورية والخاملة.

6) يُتطلب إرسال أوامر الإدارة عبر منصة إدارة الموارد الافتراضية في نفق آمن.

7) يوصى بكبح الأوامر المميزة عند تنفيذها عن بُعد.

8) يُتطلب عزل وحدات الموارد الافتراضية غير القانونية والتخلص منها بشكل مناسب لتقليل التأثير اللاحق على الموارد الافتراضية بأكملها إلى أدنى حد.

9) يُتطلب تقديم قدرة كشف الشفرة الخبيثة والتخلص من هذه الشفرة.

10) يوصى بانتقال سياسة الأمن بعد الانتقال المتزامن لوحدات الموارد الافتراضية.

11) يُتطلب تنفيذ برمجيات الأمن التصحيحية أو تشكيلة تعزيز الأمن في الوقت المناسب بمجرد اكتشاف ثغرة أمنية في مكونات إدارة الموارد الافتراضية (مثل المشرف على الآلات الافتراضية، ومحرك الحاوية، ومكونات الإدارة، وما إلى ذلك)، وأن يجري تحديثها باستمرار.

12) يُتطلب تقديم إدارة الأعطال للحفاظ على استمرارية الخدمة العليا، بحيث يمكن نقل وحدات الموارد الافتراضية على آلة مضيفة متعطلة إلى آلة مضيفة أخرى في الوقت المناسب.

13) يُتطلب تسجيل جميع العمليات والأحداث على منصة إدارة الموارد الافتراضية للتتبع والتدقيق اللاحقين.

2.10 متطلبات أمن المورد المادي

تتضمن الموارد المادية موارد العتاد، مثل الحواسيب ومعدات الشبكة ومكونات التخزين وغيرها من عناصر البنية التحتية للحوسبة المادية التي يحتاجها مقدم الخدمة السحابية لتشغيل وإدارة خدمات IaaS المقدَّمة إلى عملاء الخدمة السحابية.

1.2.10 متطلبات أمن البيئة المادية

ترد في المرجع [ISO/IEC 27002] متطلبات أمن البيئة المادية للبنية التحتية كخدمة.

1.1.2.10 متطلبات أمن الموارد المادية

تتضمن الموارد المادية موارد العتاد، مثل البنية التحتية للتوصيل الشبكي المادي وأجهزة التخزين والآلات المضيفة ومطاريف الإدارة وعناصر البنية التحتية المادية الأخرى.

1) يُتطلب تقديم قدرة كشف الأعطال وتحديد مواضعها في الموارد المادية (مثل معدات التوصيل الشبكي، والآلات المضيفة، وأجهزة التخزين، وما إلى ذلك) للحفاظ على تيسر وموثوقية البنية التحتية المادية الأساسية.

2) يوصى بإمكانية كشف تغير الموارد المادية ووسمها في الوقت المناسب.

3) يوصى بإمكانية تقديم قدرة استعادة البيانات عند تعطل بعض المكونات المادية.

4) يُتطلب تقديم قدرة القدرة الدفاعية لمنصة IaaS ضد الحرمان من الخدمة الموزَّع.

5) يُتطلب تقسيم شبكة البنية التحتية إلى ميادين أمن شبكة مختلفة، معزولة منطقياً عن بعضها البعض.

6) يُتطلب تنفيذ آليات الكشف الخاصة بمراقبة حركة الشبكة وسلوك التسلل، مع نشر أجهزة الحماية على حدود الشبكة بما في ذلك إدارة الهوية والنفاذ (IAM)، ونظام منع التسلل (IPS)، وجدار الحماية، وما إلى ذلك

7) يوصى بإمكانية كشف سلوكيات الهجوم الصادرة عن الشبكة التي تشَن من مورد IaaS، ومنعها.

8) يُتطلب تقديم قدرة كشف الشفرة الضارة والتخلص منها، خاصة لمطاريف الإدارة والآلات المضيفة ومخدمات التطبيقات الأخرى.

9) يُتطلب تنفيذ خط أساس لسياسة الأمن بحيث لا يتمكن من النفاذ إلى منصة IaaS سوى المطاريف والمخدمات الملبية لسياسات الأمن.

10) يُتطلب تسجيل جميع العمليات والأحداث الجارية على الموارد المادية للتتبع والتدقيق لاحقاً.

11 متطلبات إدارة الأمن

تتولى إدارة الأمن مسؤولية تطبيق الضوابط المتعلقة بالأمن لتخفيف التهديدات الأمنية في بيئات الحوسبة السحابية. وتشمل المكونات الوظيفية لإدارة الأمن جميع المرافق الأمنية اللازمة لدعم الخدمات السحابية.

وتشمل المكونات الوظيفية لإدارة الأمن ما يلي:

- إدارة الهوية ومراقبة النفاذ؛
- التدقيق الأمني؛
- إدارة نقاط الضعف؛
- الاستجابة للطوارئ؛
- التعافي من الأعطال الكبرى؛
- النسخ الاحتياطي.

1.11 إدارة الهوية والتحكم في النفاذ

ينبغي أن تقدم منصة IaaS وظائف موحدة لإدارة الهوية (IdM) والتحكم في النفاذ لعملاء الخدمة السحابية وإداريي منصة IaaS.

1) يُتطلب أن ينفرد عميل الخدمة السحابية بهوية في دورة الحياة في كل خدمة من خدمات IaaS وأن ترتبط الهوية بالتدقيق الأمني. وتُتطلب إدارة هوية عميل الخدمة السحابية وصيانتها وحمايتها من النفاذ أو التعديل أو الحذف غير المأذون.

2) يُتطلب من منصة IaaS تقديم إدارة سياسة كلمة المرور لعملاء الخدمة السحابية، وهي تشمل ما يلي على سبيل المثال لا الحصر:

- يُتطلب استخدام سياسة تعقيد كلمة المرور.
- يُتطلب استخدام آلية الفترة التي تغيَّر بعدها كلمة المرور.
- يُتطلب استخدام التوليد العشوائي للمفتاح الأولي لدى عميل الخدمة السحابية، ويجب تعديل المفتاح الأولي عند تسجيل الدخول لأول مرة.

3) يوصى بأن تدعم منصة IaaS كشف الشذوذ بشأن هوية عميل الخدمة السحابية وإمكانية إرسال الإنذارات إلى عملاء الخدمة السحابية ذوي الصلة.

4) يُتطلب أن تدعم منصة IaaS الاستيقان متعدد العوامل من عملاء الخدمة السحابية، وتقنيات الاستيقان بما فيها على سبيل المثال لا الحصر كلمات المرور أو الشهادات الرقمية أو بطاقات السطح البيني (IC) أو التحقق البيومتري.

5) يُتطلب أن تُدعم استراتيجية تخويل كثيرة الجزئيات حسب عميل الخدمة السحابية وتعريف المجموعة لموارد النفاذ. ويُتطلب أن تحمي منصة IaaS كتمان وسلامة بيانات اعتماد الاستيقان الخاصة بعملاء الخدمة السحابية.

6) يُتطلب تخزين السجلات التفصيلية للاستيقان من عميل الخدمة السحابية والتخويل له والعمليات الأخرى المتعلقة بإدارة الهوية للتدقيق لاحقاً.

7) يوصى بأن تدعم منصة IaaS المقابسة مع نظام إدارة هوية عملاء الخدمة السحابية.

8) يُتطلب منح دور إداري منصة IaaS والامتيازات ذات الصلة به لحساب مختلف.

9) يُتطلب من منصة IaaS استخدام الاستيقان متعدد العوامل من الإداريين.

10) يُتطلب من منصة IaaS استخدام مبدأ تقليل صلاحيات الإداريين إلى أدنى حد.

11) يُتطلب تجفير البيانات الحساسة مثل بيانات الاستيقان، وبيانات التخويل، وما إلى ذلك، في إجراءات التخزين والنقل.

2.11 التدقيق الأمني

1) يُتطلب من منصة IaaS استخدام سجلات متنوعة للتدقيق الأمني، وتشمل السجلات على سبيل المثال لا الحصر:

- معلومات التسجيل والاستيقان من الهوية والتخويل لعملاء الخدمة السحابية وإداريي منصة IaaS.
- سجلات التشغيل والصيانة من جانب إداريي منصة البنية التحتية كخدمة عبر هذه البنية التحتية.
- سجلات التشغيل من جانب إداريي منصة البنية التحتية كخدمة عبر موارد عميل الخدمة السحابية.
- سجلات تشغيل عميل الخدمة السحابية لموارده.
- سجلات التشغيل والصيانة أثناء عملية تشغيل منصة IaaS.

2) يُتطلب من منصة IaaS تنفيذ آليات الأمن لحماية السجلات المختلفة من العبث.

3) يُتطلب أن تبقى جميع ميقاتيات الشبكة متزامنة ضمن منصة IaaS بأكملها لتسجيل النفاذ والتشغيل بشكل منتظم.

4) يجب أن تتضمن سجلات التدقيق الأمني موضوعات الحدث الأمني وكائناته ووقته وأنواعه ونتائجه.

5) يُتطلب عزل سجلات التدقيق بين عملاء الخدمة السحابية عن بعضها البعض.

6) يُتطلب أن يتمكن عميل الخدمة السحابية من جمع ومشاهدة سجلات التدقيق المتعلقة بموارده.

7) يُتطلب أن تحمى سجلات التدقيق بشكل آمن، مثل منع النفاذ غير المأذون إلى سجلات التدقيق، ومنع ما لا يُتوقع من الحذف والتعديل والتجاوز والخسارة.

8) يُتطلب من الاحتفاظ بسجلات التدقيق الإيفاء بالالتزام القانوني ومتطلبات الاحتفاظ الخاصة بعملاء الخدمة السحابية.

9) يوصى بأن تدعم منصة IaaS عميل الخدمة السحابية لاستخدام نظام أو سطح بيني للتدقيق عائد لطرف ثالث لتحقيق هدف التدقيق ضمن مسؤوليات عميل الخدمة السحابية.

3.11 إدارة نقاط الضعف

يمكن أن توجد نقاط ضعف منصة IaaS في العمليات والإدارة والتشكيلة والعتاد والبرمجيات، وما إلى ذلك.

1) يُتطلب تسجيل معلومات جميع أصول وإصدارات منصة IaaS وتحديث المعلومات بانتظام.

2) يُتطلب إنشاء آلية لتقدير نقاط الضعف، ينبغي فيها توضيح الكائنات والتواتر وتقييم استراتيجية تقدير نقاط الضعف.

3) يُتطلب إجراء تقييم لنقاط الضعف في جميع أصول منصة IaaS بانتظام، وإنشاء تقارير تقييم لنقاط الضعف وتقديم توصيات لإصلاحها.

4) تُتطلب إدارة عملية البرمجيات التصحيحية والإصلاح:

- يُتطلب تتبع التهديدات الأمنية والبرمجيات التصحيحية الأمنية الصادرة عن مختلف البائعين، وتحديد أي من البرمجيات التصحيحية ينبغي تثبيتها في منصة IaaS.
- يُتطلب اختبار البرمجيات التصحيحية الأمنية قبل التثبيت للتأكد من توافقها مع النظام والتطبيق القائمين.
- يُتطلب وضع خطة تحديث البرمجيات التصحيحية لجميع مكونات منصة IaaS، وتنفيذ تثبيت البرمجيات التصحيحية وفقاً للخطة، وإنشاء سجلات أثناء التثبيت.

5) يُتطلب إنشاء خط أساس تشكيلة الأمن لمنصة IaaS وتشكيل مكونات منصة IaaS وفقاً لخط الأساس.

6) يُتطلب إجراء تفتيش أمني أساسي لجميع أصول منصة IaaS بانتظام، ووضع تقرير تفتيش أساسي وتقديم توصيات للتصحيح.

7) يُتطلب تدقيق التغييرات في استراتيجية تشكيلة منصة IaaS للتحقق من صحة كل بند في تشكيلة ومن اتساقه واكتماله وفعاليته، والتأكد من أن تغييرات التشكيلة لا تجلب ثغرات أمنية جديدة.

4.11 الاستجابة للطوارئ

تتوافق اعتبارات الاستجابة للطوارئ في البنية التحتية كخدمة مع ما يرد في الفقرة 9.8 من التوصية [ITU-T X.1642].

5.11 التعافي من الكوارث

ينبغي أن تتوافق اعتبارات التعافي من الكوارث في البنية التحتية كخدمة مع اللوائح المشتركة القائمة لتكنولوجيا المعلومات، مثل المعيار [ISO/IEC 27031]. بيد أن التعافي من الكوارث في البنية التحتية كخدمة، باعتباره تكنولوجيا سريعة النمو، ينبغي أن يأخذ في الاعتبار أيضاً:

1) تعريف كائنات التعافي من الكوارث لكل عميل خدمة سحابية. ويُتطلب بدء تحليل التأثير التجاري (BIA) لتحديد كائنات التعافي من الكوارث في مصالح الأعمال المختلفة، وهو يستند إلى التعرف على المكونات الرئيسية والمخاطر الأمنية الرئيسية على منصة IaaS. ويمكن تعريف كائنات التعافي من الكوارث حسب الأولويات، وRPO/RTO، وما إلى ذلك. وتحدد كائنات التعافي من الكوارث المختلفة ما يقابلها من اتفاق مستوى الخدمة (SLA) ومعمارية الخدمة، بما في ذلك تكنولوجيا التيسر العالي عبر مراكز البيانات الافتراضية (VDC) البعيدة، والنسخ الاحتياطي للبيانات العابر للمناطق، وما إلى ذلك.

2) النسخ الاحتياطي للأنظمة والبيانات بانتظام. ويُتطلب دعم قدرة تخزين البيانات العابر للمناطق وتحمُّل الكوارث. علاوةً على ذلك، ينبغي تقديم أنواع النسخ الاحتياطي على مستوى النظام والنسخ الاحتياطي على مستوى البيانات لمستأجري منصة IaaS وكذلك القدرة المقابلة على التعافي من الكوارث التي يمكن أن تساعد مقدمي الخدمة السحابية وعملاء الخدمة السحابية على القيام بتجاوز الخلل. وبالنسبة لعملاء الخدمة السحابية، يمكنهم نسخ البيانات احتياطياً حتى لدى مقدم خدمة سحابية مختلف بانتظام، لتجنب خطر الإنهاء بعد انقضاء وقت طويل لدى مقدم خدمة سحابية واحد.

3) التحقق من صحة خطة التعافي من الكوارث بانتظام. وعلى الرغم من أن أنظمة وبيانات عملاء الخدمة السحابية يمكن أن تحافظ على ثباتها نسبياً، إلا أن مخاطر أمنية جديدة قد تظهر أيضاً من خلال تحديثات البنية التحتية التي يطلقها مقدمو الخدمة السحابية. لذلك، ينبغي إجراء تمارين التعافي من الكوارث بانتظام، وينبغي تسجيل المعلومات الأساسية بما في ذلك تيسر خطط التعافي من الكوارث وسلامتها وصلاحيتها، والمشاكل والحلول المقابلة في هذه العملية وما إلى ذلك.

4) تقييم المخاطر بانتظام. فلدعم استمرارية أعمال عملاء الخدمة السحابية، ينبغي أن يقيِّم مقدمو الخدمة السحابية المخاطر الأمنية التي يمكن أن تؤثر على خطة استمرارية أعمال عملاء الخدمة السحابية، والتي تشمل تعطل خدمة IaaS، وانقطاع الشبكة بين مقدم الخدمة السحابية وعميل الخدمة السحابية، وإنهاء الخدمات السحابية، وما إلى ذلك، وينبغي الاجتهاد في إبلاغ النتائج إلى عملاء الخدمة السحابية. علاوةً على ذلك، ينبغي الإبلاغ مقدماً عن الاستجابة للطوارئ، وخطط وأنشطة التعافي من الكوارث لدعم استمرارية أعمال عميل الخدمة السحابية، بل وتعديلها وفقاً لمتطلبات عملاء الخدمة السحابية.

6.11 النسخ الاحتياطي

تتوافق اعتبارات النسخ الاحتياطي في البنية التحتية كخدمة مع ما يرد في الفقرة 10.8 من التوصية [ITU-T X.1642].

بيبليوغرافيا

[b-ITU-T X.1601] Recommendation ITU-T X.1601(2015), *Security framework for cloud computing*.

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

[b-NIST 500-291] NIST SP 500-291,2011, *NIST Cloud Computing Standards Roadmap*.

[b-NIST-SP-800-30] NIST Special Publication 800-30, 2012, *Guide for Conducting Risk Assessments*.

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