الاتحـــــــــــاد الدولـــــــــــي للاتصـــــــــــالات

ITU-T

قطاع تقييس الاتصالات
في الاتحاد الدولي للاتصالات

X.1642
(2016/03)

السلسلة X: شبكات البيانات والاتصالات بين الأنظمة المفتوحة ومسائل الأمن

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

مبادئ توجيهية من أجل الأمن التشغيلي للحوسبة السحابية

التوصية ITU-T X.1642

توصيات السلسلة X الصادرة عن قطاع تقييس الاتصالات

شبكات البيانات والاتصالات بين الأنظمة المفتوحة ومسائل الأمن

الشبكات العمومية للبيانات	X.199–X.1
التوصيل البيني للأنظمة المفتوحة	X.299–X.200
التشغيل البيني للشبكات	X.399–X.300
أنظمة معالجة الرسائل	X.499–X.400
الدليل	X.599–X.500
التشغيل البيني لأنظمة التوصيل OSI ومظاهر النظام	X.699–X.600
إدارة التوصيل البيني للأنظمة المفتوحة (OSI)	X.799–X.700
الأمن	X.849–X.800
تطبيقات التوصيل البيني للأنظمة المفتوحة (OSI)	X.899–X.850
المعالجة الموزعة المفتوحة	X.999–X.900
أمن المعلومات والشبكات	
الجوانب العامة للأمن	X.1029–X.1000
أمن الشبكة	X.1049–X.1030
إدارة الأمن	X.1069–X.1050
القياسات البيومترية عن بُعد	X.1099–X.1080
تطبيقات وخدمات آمنة	
أمن البث المتعدد	X.1109–X.1100
أمن الشبكة المحلية	X.1119–X.1110
أمن الخدمات المتنقلة	X.1139–X.1120
أمن الويب	X.1149–X.1140
بروتوكولات الأمن	X.1159–X.1150
الأمن بين جهتين نظيرتين	X.1169–X.1160
أمن معرفات الهوية عبر الشبكات	X.1179–X.1170
أمن التلفزيون القائم على بروتوكول الإنترنت	X.1199–X.1180
أمن الفضاء السيبراني	
الأمن السيبراني	X.1229–X.1200
مكافحة الرسائل الاقتحامية	X.1249–X.1230
إدارة الهوية	X.1279–X.1250
تطبيقات وخدمات آمنة	
اتصالات الطوارئ	X.1309-X.1300
أمن شبكات المحاسيس واسعة الانتشار	X.1339–X.1310
التوصيات المتعلقة بالبنية التحتية للمفاتيح العمومية	X.1349–X.1340
تبادل معلومات الأمن السيبراني	
نظرة عامة عن الأمن السيبراني	X.1519–X.1500
تبادل مواطن الضعف/الحالة	X.1539–X.1520
تبادل الأحداث/الأحداث العارضة/المعلومات الحدسية	X.1549–X.1540
تبادل السياسات	X.1559–X.1550
طلب المعلومات الحدسية والمعلومات الأخرى	X.1569–X.1560
تعرف الهوية والاكتشاف	X.1579–X.1570
التبادل المضمون	X.1589–X.1580
أمن الحوسبة السحابية	
نظرة عامة على أمن الحوسبة السحابية	X.1601–X.1600
تصميم أمن الحوسبة السحابية	X.1639–X.1602
أفضل الممارسات ومبادئ توجيهية بشأن أمن الحوسبة السحابية	**X.1659–X.1640**
تنفيذ أمن الحوسبة السحابية	X.1679–X.1660
أمن أشكال أخرى للحوسبة السحابية	X.1699–X.1680

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

التوصية ITU-T X.1642

مبادئ توجيهية من أجل الأمن التشغيلي للحوسبة السحابية

ملخص

تقدم التوصية ITU-T X.1642 مبادئ توجيهية عامة للأمن التشغيلي للحوسبة السحابية من منظور مقدمي الخدمات السحابية (CSP). وهي تحلل المتطلبات والمقاييس الأمنية لتشغيل الحوسبة السحابية. كما تقدم التوصية مجموعة من التدابير الأمنية وأنشطة أمنية مفصلة من أجل التشغيل اليومي والصيانة لمساعدة مقدمي الخدمات السحابية في الحد من المخاطر الأمنية ومواجهة التحديات الأمنية الخاصة بتشغيل الحوسبة السحابية.

التسلسل التاريخي

الطبعة	التوصية	تاريخ الموافقة	لجنة الدراسات	معرف الهوية الفريد*
1.0	ITU-T X.1642	2016-03-23	17	11.1002/1000/12616

مصطلحات أساسية

الحوسبة السحابية، الأمن التشغيلي، بند الأمن في اتفاق مستوى الخدمة (SLA).

* 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 "يجب" وصيغ ملزمة أخرى مثل فعل "ينبغي" 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.1642

مبادئ توجيهية من أجل الأمن التشغيلي للحوسبة السحابية

1 مجال التطبيق

توضح هذه التوصية المسؤوليات الأمنية بين مقدمي الخدمات السحابية (CSP) وعملاء الخدمات السحابية (CSC)، وتحلل متطلبات وفئات المقاييس الأمنية للأمن التشغيلي المتعلق بالحوسبة السحابية. وهي تحدد مجموعة من الإجراءات الأمنية والأنشطة الأمنية المفضّلة من أجل التشغيل اليومي والصيانة للخدمات والبنى التحتية المتعلقة بالحوسبة السحابية من منظور مقدمي الخدمات السحابية، وذلك لتلبية متطلبات الأمن التشغيلي للحوسبة السحابية.

وستفيد هذه التوصية مقدمي الخدمات السحابية في الحد من المخاطر التشغيلية. والجمهور الذي تستهدفه هم مقدمو الخدمات السحابية، من قبيل مشغلي الاتصالات التقليديين ومقدمي خدمات الإنترنت (ISP).

2 المراجع

لا يوجد.

3 التعاريف

1.3 مصطلحات معرفة في وثائق أخرى

تستخدم هذه التوصية المصطلحات التالية المعرَّفة في وثائق أخرى:

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

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

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

4.1.3 شريك في الخدمة السحابية [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 [b-ITU-T Y.3500]: طرف يتيح توافر الخدمات السحابية.

6.1.3 البنية التحتية كخدمة (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 تعدد الشاغلين [b-ITU-T Y.3500]: توزيع الموارد المادية أو الافتراضية بحيث يتم عزل الشاغلين المتعددين وحساباتهم وبياناتهم عن بعضهم البعض، ويكون النفاذ غير ممكن فيما بين بعضهم البعض.

8.1.3 الشبكة كخدمة (NaaS) [b-ITU-T Y.3500]: فئة من الخدمات السحابية تكون فيها القدرة المقدمة لعميل الخدمة السحابية متمثلة في قدرة توصيلية النقل والقدرات المتصلة بالشبكات.

9.1.3 الطرف [b-ISO 27729]: شخص طبيعي أو اعتباري، اكتسب الشخصية الاعتبارية أم لم يكتسبها، أو مجموعة تضم كليهما.

10.1.3 المنصات كخدمة (PaaS) [b-ITU-T Y.3500]: فئة من الخدمات السحابية تكون فيها القدرات السحابية المقدمة لعميل الخدمة السحابية من نوع قدرات المنصة.

11.1.3 تحدٍّ أمني [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".

12.1.3 ميدان أمني [b-ITU-T X.810]: مجموعة عناصر وسياسة أمن وسلطة أمن ومجموعة أنشطة ذات صلة بالأمن تدار فيها العناصر من أجل الأنشطة المحددة طبقاً لسياسة الأمن، وتعمد سلطة الأمن إلى تطبيق سياسة الأمن بالنسبة لميدان الأمن.

13.1.3 حادث أمني [b-ITU-T E.409]: الحادث الأمني هو أي حدث سلبي يمكن أن تُهدَّد فيه بعض جوانب الأمن.

14.1.3 اتفاق مستوى الخدمة (SLA) [b-ISO/IEC 20000-1]: اتفاق موثّق مُبرم بين مقدم الخدمة والعميل تُحدَّد فيه الخدمات وأهداف الخدمات.

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

16.1.3 شاغل [b-ITU-T Y.3500]: مستعمل واحد أو أكثر من مستعملي الخدمات السحابية الذين يتقاسمون مجموعة من الموارد المادية والافتراضية.

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

18.1.3 نقطة ضعف [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 يوجد.

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)*

CCTV الدوائر التلفزيونية المغلقة *(Closed Circuit TeleVision)*

CPU وحدة المعالجة المركزية *(Central Processing Unit)*

CSC عميل الخدمة السحابية *(Cloud Service Customer)*

CSN شريك الخدمة السحابية *(Cloud Service Partner)*

CSP مقدم الخدمة السحابية *(Cloud Service Provider)*

DB قاعدة بيانات *(Database)*

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

DLP منع تسرُّب البيانات *(Data Leakage Prevention)*

DoS الحرمان من الخدمة *(Denial of Service)*

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)*

IDS نظام كشف التسلّل *(Intrusion Detection System)*

IP بروتوكول الإنترنت *(Internet Protocol)*

IPS نظام منع التسلل *(Intrusion Prevention System)*

ISP مقدم خدمة الإنترنت *(Internet Service Provider)*

IT تكنولوجيا المعلومات *(Information Technology)*

JIT في الوقت المناسب *(Just In Time)*

LDAP بروتوكول النفاذ الخفيف إلى الدليل *(Lightweight Directory Access Protocol)*

NaaS الشبكة كخدمة *(Network as a Service)*

OS نظام التشغيل *(Operating System)*

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)*

SMS خدمة الرسائل القصيرة *(Short Message Service)*

SSO تسجيل وحيد للدخول *(Single Sign-On)*

VDC مركز البيانات الافتراضية *(Virtual Data Centre)*

VM آلة افتراضية *(Virtual Machine)*

5 الاصطلاحات

لا يوجد.

6 لمحة عامة

نظراً إلى التوسع السريع لسوق الحوسبة السحابية وإنشاء السلاسل الصناعية، لا تزال القضايا الأمنية تشكل موضوعاً رئيسياً ومهماً لا يمكن تجاهله. وتواجه أنظمة الحوسبة السحابية تحديات أكثر بالمقارنة مع التحديات التي تواجهها الأنظمة التقليدية لتكنولوجيا المعلومات (IT)، لأنها أكثر تعقيداً، وقد خُزنت كميات هائلة من البيانات الخاصة بالمستخدمين في الحيز السحابي. وتشكل الحماية الأمنية والخصوصية على السواء أهم العوامل عندما يقوم العملاء بتقييم استخدام خدمات الحوسبة السحابية.

وستقدم المزيد من الخدمات السحابية، وقد أصبحت الحاجة إلى الأساليب التي تضمن موثوقية هذه الخدمات أكثر إلحاحاً. ولذلك، تقتضي الضرورة إجراء تحقيق دقيق بشأن الأمن التشغيلي للحوسبة السحابية لتوفير مبادئ توجيهية لصالح مقدمي الخدمات السحابية (CSP). ويمكن للمبادئ التوجيهية أن تساعد مقدمي الخدمات السحابية على الحد من المخاطر الأمنية الناجمة عن التشغيل السيء والإعداد غير المعقول للأعمال، وما إلى ذلك، وتحسين المستوى الأمني الشامل للعمليات فيما يتعلق بخدمات الحوسبة السحابية.

وفيما يلي التحديات الأمنية الرئيسية للأمن التشغيلي من منظور مقدمي الخدمات السحابية:

1) التحديات التي تواجه صيانة البنية التحتية للحوسبة السحابية: متى زودت الحوسبة السحابية المستخدمين بالبنية التحتية لتكنولوجيا المعلومات أو بالمنصات أو البرمجيات كخدمة، يصبح التقديم المأمون للخدمات السحابية واستقرارها وموثوقيتها شرطاً لا غنى عنه لممارسة الأعمال. ومن أجل كفالة عدم انقطاع الخدمة المقدمة إلى العملاء، ينبغي ضمان البنية التحتية لنظام الحيز السحابي من أجل تشغيل موثوق ومستقر، وينبغي اتخاذ الاحتياطات اللازمة لحماية سلامة وخصوصية معلومات المستخدم. وحتى في حالة حدوث عطل صغير، يمكن أن يواجه العديد من عملاء الخدمات السحابية صعوبات مثل تعطل الأعمال أو ضياع البيانات. وينبغي لمقدمي الخدمات السحابية أن يفكروا بجدية في كيفية تحديد مكان العطل بسرعة والانتقال أوتوماتياً إلى النظام الاحتياطي بسلاسة لحماية تيسر خدمة العملاء.

2) التحديات التي تواجه أسلوب إدارة الحوسبة السحابية: إن خصائص الحوسبة السحابية، من قبيل الخدمات متعددة المناطق، وقدرات الحوسبة الجبارة، والفصل بين إدارة البيانات وملكيتها، تميزها عن الخدمات التقليدية لتكنولوجيا المعلومات. وتتطلب هذه التحديات الإدارة الفعّالة والتعاون بين الشبكات الفرعية لكي يتسنى لمقدمي الخدمات السحابية حل المشاكل الأمنية. وبالنسبة إلى مقدمي الخدمات السحابية، ستكون هناك حاجة إلى بعض الإجراءات التقنية اللازمة، مثل إدارة تشكيلة الأمن وما إلى ذلك، وإلى توزيع صحيح لسلطة الإدارة، ومجموعة من القواعد والعمليات للإدارة الفعّالة، من أجل منع تسرب بيانات المستخدم. وعلى سبيل المثال، ينبغي لمقدمي الخدمات السحابية أن يتخذوا التدابير اللازمة للحيلولة دون تجاوز المشرفين الداخليين لصلاحيتهم وذلك لمنع المستخدمين من إساءة استخدام موارد الحوسبة السحابية.

وبوجه عام، ومن أجل تحقيق الأمن الكامل للتطبيقات السحابية المشغلة على البنية التحتية السحابية، ينبغي لمقدمي الخدمات السحابية أن يعتمدوا مختلف الأساليب التكنولوجية وآليات الإدارة لا للحفاظ على أمن البنية التحتية السحابية واستقرارها وتوافرها فحسب، بل أيضاً لحماية استمرار الأعمال وبيانات المستخدم للخدمات السحابية العاملة.

7 متطلبات بند الأمن في اتفاق مستوى الخدمة

يعتبر بند الأمن في اتفاق مستوى الخدمة (SLA) العامل الحاسم بالنسبة إلى مقدمي الخدمات السحابية للحصول على ثقة المستخدم. وينبغي وصف العلاقة القائمة بين عملاء الخدمات السحابية ومقدمي الخدمات السحابية، من قبيل المسؤولية الأمنية، بوضوح في بند الأمن في اتفاق مستوى الخدمة. وينبغي لمقدمي الخدمات السحابية أن يركزوا إجراءاتهم الأمنية التشغيلية على الوفاء بالمتطلبات التي حددها بند الأمن في اتفاق مستوى الخدمة.

1.7 المسؤولية الأمنية بين مقدمي الخدمات السحابية و عملاء الخدمات السحابية

ينبغي تحديد مسؤوليات مقدمي الخدمات السحابية وعملاء الخدمات السحابية فيما يتعلق بأمن الحوسبة السحابية وفقاً لقدرات التحكم المختلفة في البنية التحتية للحوسبة السحابية ومواردها.

وترتبط المسؤوليات الأمنية ارتباطاً وثيقاً بأسلوب الخدمة السحابية، لأن هذا الأسلوب يعكس القدرة على التحكم في الموارد في البيئة السحابية بالنسبة إلى مقدمي الخدمات السحابية وعملائها. وعلى سبيل المثال، وبالمقارنة مع المنصة كخدمة (PaaS) أو البنية التحتية كخدمة (IaaS)، ينبغي لموردي الخدمات السحابية في البرمجيات كخدمة (SaaS) أن يضطلعوا بالمزيد من المسؤوليات الأمنية كما لو أن قدرة أقوى للتحكم في الموارد في المتناول.

وفيما يتعلق بأسلوب خدمة البنية التحتية كخدمة، يوفر مقدمو الخدمات السحابية خدمات البنية التحتية، من قبيل مركز البيانات الافتراضية (VDC) الذي يشمل المخدّمات المستضافة وموارد التخزين وأدوات الشبكة والإدارة. وتشمل المسؤوليات الأمنية الأساسية لمقدمي الخدمات السحابية الأمن المادي وأمن الشبكة وأمن النظام الأساسي وموثوقية البنية السحابية برمتها. وينبغي أن يكون عملاء الخدمات السحابية مسؤولين عن جميع القضايا الأمنية التي تتعدى مستوى البنية التحتية السحابية التي يشترونها، مثل أمن نظام التشغيل الخاص بالضيوف (OS) وبرمجيات التطبيق، وما إلى ذلك.

وفيما يتعلق بأسلوب خدمة المنصات كخدمة، يوفر مقدمو الخدمات السحابية بيئة تطوير واختبار ونشر البرمجيات المبسطة والموزعة. وينبغي أن يكون موردو الخدمات السحابية مسؤولين عن أمن السطح البيني لبرمجة التطبيقات (API) لبيئة التطبيق، وأمن البرمجيات الوسيطة، وتوافر المنصة السحابية، إلخ.، فضلاً عن أمن البنية التحتية الأساسية. ومن ناحية أخرى، ينبغي أن يكون عملاء الخدمات السحابية مسؤولين عن أمن خدمات التطبيقات العاملة في بيئة المنصة السحابية.

وفيما يتعلق بأسلوب خدمة البرمجيات كخدمة، ينبغي لمقدمي الخدمات السحابية أن يضمنوا الأمن الشامل لطبقة التطبيقات من طبقة البنية التحتية، وأن يحافظ عملاء الخدمات السحابية على أمن المعلومات المتعلقة بهم، من قبيل أمن إدارة الهوية (IdM) ومنع تسرب كلمة السر، وما إلى ذلك.

بالإضافة إلى ذلك، ينبغي لعملاء الخدمات السحابية مراعاة القضايا الأمنية المتعلقة بالمطاريف التي يستخدموها للنفاذ إلى الحيز السحابي.

2.7 متطلبات بند الأمن في اتفاق مستوى الخدمة

1.2.7 متطلبات عامة

ينبغي لبند الأمن في اتفاق مستوى الخدمة أن يحدد بوضوح مصطلحات الأمن المتعلقة بالخدمات السحابية، فضلاً عن مسؤوليات مقدمي الخدمات السحابية وعملاء الخدمات السحابية والتزاماتهم.

ومن منظور عملاء الخدمات السحابية، ينبغي أن يكون في مقدور العملاء تحديد متطلباتهم فيما يتعلق ببند الأمن في اتفاق مستوى الخدمة. ويمكن لبند الأمن في اتفاق مستوى الخدمة أن يساعدهم على التأكد من أن مقدمي الخدمات السحابية يوفرون الحماية الكافية لأصولهم ومواردهم وخدماتهم المعلوماتية حسب الطلب أثناء التوقف والاستخدام والتنقل، وأنه قد تم تنفيذ آليات تصحيحية للامتثال للوائح المتعلقة بخصوصية البيانات المرتبطة بولايتهم القضائية.

ومن منظور مقدمي الخدمات السحابية، يحدد بند الأمن في اتفاق مستوى الخدمة متطلبات أمن الخدمة السحابية المقدمة ومصطلحاته القابلة للقياس، التي يمكن لعملاء الخدمات السحابية أن يضطلعوا بتقييمها ومقارنتها وتعديلها. وينبغي لمقدمي الخدمات السحابية أن ينفذوا مجموعة من الآليات التكنولوجية والإدارية المناسبة لتحسين موثوقية وأمن الخدمات السحابية، والوفاء بمتطلبات بند الأمن في اتفاق مستوى الخدمة، الذي يمكن أن يحصل في نهاية المطاف على ثقة عملاء الخدمات السحابية. وقد يكون لدى الخدمات السحابية أنواع مختلفة من اتفاقات مستوى الخدمة بسبب محتوى الخدمات ودرجة الخدمة وحتى المنطقة التي تقدم فيها الخدمات، ولكن ينبغي للمتطلبات الدنيا لبند الأمن في اتفاق مستوى الخدمة أن تلبي المتطلبات القانونية والتنظيمية، فضلاً عن متطلبات المعايير الصناعية ذات الصلة.

ويمكن لمقدمي الخدمات السحابية وعملاء الخدمات السحابية أن يتفاوضوا على المتطلبات المحددة لبند الأمن في اتفاق مستوى الخدمة استناداً إلى المتطلبات المعدلة لعملاء الخدمات السحابية وقدرتهم على التحكم في الموارد. وبالنسبة إلى مقدمي الخدمات السحابية، ينبغي الإشارة بوضوح إلى بنود إخلاء المسؤولية في أي عقد تجاري أو وصف منتج لتجنب المنازعات التي لا داعي لها أو المخاطر الأمنية، بحيث لا تقع المسؤولية في حالة القوة القاهرة على عاتق مقدمي الخدمات السحابية.

2.2.7 عناصر بند الأمن في اتفاق مستوى الخدمة

يشمل بند الأمن في اتفاق مستوى الخدمة، دون أن يقتصر على ذلك، العناصر التالية.

1.2.2.7 استمرار الأعمال

ينبغي لمقدمي الخدمات السحابية أن يوفروا الحماية الكافية في حالة وقوع كارثة من صنع الإنسان أو كارثة طبيعية لضمان إتاحة الخدمة واستمرار الأعمال. وترد فيما يلي البنود والمتطلبات المفصلة.

1) توافر الخدمة

النسبة المئوية للوقت الذي يمكن الاستفادة في إطاره من الخدمة في فترة زمنية معينة. وفيما يتعلق بخدمة سحابية معينة، ينبغي ألا تكون شروط قدرات الخدمة أقل من الخدمات التقليدية لتكنولوجيا المعلومات والاتصالات (ICT) بوجه عام.

2) متوسط وقت الاستعادة

الوقت اللازم لاستعادة البيانات المفقودة أو استئناف الخدمة بعد حدوث عطل أو أعطال كبرى أخرى.

2.2.2.7 حماية أمن البيانات

ينبغي أن يكون لدى مقدمي الخدمات السحابية برنامج حماية شامل لحماية بيانات عملاء الخدمات السحابية وغيرها من المعلومات الخصوصية، وينبغي لمقدمي الخدمات السحابية وعملاء الخدمات السحابية أن يتوصلوا إلى اتفاق بشأن الآليات والمتطلبات المفصلة.

1) الأمن المادي لخدمة التخزين

ينبغي لمقدمي الخدمات السحابية أن ينفذوا التدابير اللازمة لضمان الأمن المادي لخدمة التخزين، من قبيل حارس المدخل ونظام الوقاية من الحريق ونظام احتياطي للتزويد بالطاقة، وما إلى ذلك.

2) حماية وسط تخزين البيانات

ينبغي لمقدمي الخدمات السحابية أن يتخذوا التدابير اللازمة لتوفير الحماية، من قبيل تعزيز الأجهزة وتحسين البرمجيات التصحيحية وما إلى ذلك، لتعزيز أمن وسط تخزين البيانات.

3) تشفير البيانات

ينبغي الإشارة إلى البيانات التي تم تشفيرها في عملية التخزين أو الإرسال، وتفاصيل خوارزميات التشفير.

4) التحكم في النفاذ إلى البيانات

ينبغي تحديد التدابير المتخذة للتحكم في النفاذ إلى المعلومات للحيلولة دون النفاذ غير المشروع.

5) عزل البيانات

من الجدير بالملاحظة أن بيانات مختلف عملاء الخدمات السحابية معزولة منطقياً أو مادياً.

6) حذف البيانات

تشمل ضمان حذف البيانات. وينبغي التأكد من أن البيانات قد حذفت نهائياً قبل توزيع الموارد لعملاء آخرين للخدمات السحابية.

7) تخزين نسخ احتياطية للبيانات

تشمل أحكام هدف نقطة الاستعادة (RPO) وأهداف وقت الاستعادة (RTO) وسياسة الاحتفاظ بالبيانات والجمع بين تخزين نسخ احتياطية في الموقع وخارجه، إلخ.

8) التدقيق في العمليات التي أجريت على البيانات

ينبغي لمقدمي الخدمات السحابية أن يدققوا في العمليات التي أجريت على بيانات عملاء الخدمات السحابية وأن يكونوا قادرين على كشف العمليات غير العادية؛ وينبغي أن يكون المدقق معتمداً حتى يكون مؤهلاً لإجراء عملية التدقيق.

9) تطابق البيانات

ينبغي أن تمتثل عملية جمع البيانات ونقلها وتداولها وتخزينها وإتلافها للوائح والقوانين السارية في الولاية القضائية لعملاء الخدمات السحابية. وعلى غرار ذلك، ينبغي أيضاً أن تمتثل متطلبات الاحتفاظ بالبيانات لوقت الاحتفاظ الذي تسمح به مختلف القيود القضائية.

3.2.2.7 مواجهة حالات الطوارئ

ينبغي لمقدمي الخدمات السحابية أن يوفروا خدمات الاتصال الهاتفي المباشر لتقديم خدمة الإبلاغ عن الأعطال، بحيث تكون متاحة 5*8 أو 7*24. بالإضافة إلى ذلك، ينبغي أن تتضمن مؤشرات الخدمة وقتاً لقبول العطل ووقتاً لتصحيح الأخطاء، وما إلى ذلك.

4.2.2.7 التدابير الأمنية

ينبغي لمقدمي الخدمات السحابية أو يوفروا التدابير الأمنية المناسبة للبنية التحتية للحوسبة السحابية برمتها.

1) تدابير بشأن التمثيل الافتراضي للحوسبة

ينبغي لمقدمي الخدمات السحابية أن ينفذوا التدابير المتاحة لتوفير خدمة تفتيش التدفق أو جدار الحماية الافتراضية أو ميزات أمنية أخرى في طبقة المشرف الأعلى، مما قد يبقي سلوك الآلات ضمن الحيز الافتراضي (VM) جلياً ويمكن للجهات الإدارية التحكم به.

2) عزل الشبكة والميدان

ينبغي لمقدمي الخدمات السحابية أن ينفذوا تدابير عزل الشبكة والميدان، من قبيل جدار الحماية وسياسة قائمة التحكم في النفاذ (ACL) في المسيّرات ومراقبي الميادين للحفاظ على العزلة الصارمة لمختلف عملاء الخدمات السحابية.

3) امتياز النفاذ

ينبغي لمقدمي الخدمات السحابية أن ينفذوا التدابير اللازمة، من قبيل النفاذ في الوقت المناسب (JIT)، لضمان امتياز النفاذ.

4) الاستيقان

ينبغي لمقدمي الخدمات السحابية أن ينفذوا أساليب استيقان محكمة، من قبيل الاستيقان متعدد العوامل والاستيقان بالبصمة، وما إلى ذلك، لتعزيز أمن الاستيقان.

5) تدابير لتأمين الحركة في الشبكة

ينبغي لمقدمي الخدمات السحابية أن ينفذوا التدابير المتاحة لمقاومة الحرمان من الخدمة (DoS)/الهجمات الموزعة للحرمان من الخدمة (DDoS) والالتفاف على اكتظاظ الشبكة ونشر أنظمة كشف أو منع التسلل لمقاومة عمليات التسلل إلى الشبكة.

6) تدابير ضد البرمجيات الضارة

ينبغي لمقدمي الخدمات السحابية أن ينفذوا التدابير المتاحة لمنع العدوى بالبرمجيات الضارة أو بالفيروسات.

7) الارتقاء بالبرمجيات التصحيحية

ينبغي لمقدمي الخدمات السحابية أن ينفذوا بانتظام عمليات الارتقاء بالبرمجيات التصحيحية وبالإصدارات بالنسبة إلى برمجيات التمثيل الافتراضي ونظام التشغيل وقاعدة البيانات (DB) لتواكب المستجدات.

5.2.2.7 التدقيق الأمني

ينبغي لمقدمي الخدمات السحابية أن يقوموا بعمليات تدقيق أمنية منتظمة في نظام الحوسبة السحابية بأكملها. ويمكن أن ينفذ عملية التدقيق فريق تدقيق مستقل داخلي أو مدققين تابعين لأطراف ثالثة (بوصفهم شركاء الخدمات السحابية (CSN)). وينبغي أن تكون نتائج التدقيق جلية بما يكفي لعملاء الخدمات السحابية.

6.2.2.7 المراقبة الأمنية من أجل تحسين اتفاق مستوى الخدمة (SLA)

ينبغي لمقدمي الخدمات السحابية أن يوفروا آلية لمراقبة المعلمات الكمية للخدمات من أجل تحسين اتفاق مستوى الخدمة.

1) أشياء المراقبة

تحديد أشياء المراقبة، مثل استعمال وحدة المعالجة المركزية (CPU) والإنذارات الأمنية وما إلى ذلك. كما ينبغي الإشارة بوضوح إلى ظروف الإطلاق.

2) التبليغ عن الأحداث الأمنية

ينبغي النص على أسلوب ووقت التبليغ عن الأحداث الأمنية. ويشمل أسلوب التبليغ البريد الإلكتروني أو الهاتف أو الرسائل القصيرة أو الطرق الأخرى التي تفاوض بشأنها مقدمو الخدمات السحابية وعملاء الخدمات السحابية. ووقت التبليغ يعني متوسط الوقت اعتباراً من وقوع الحدث إلى وقت إخطار عميل الخدمات السحابية. ويمكن لمقدمي الخدمات السحابية أن يوفروا القدرات المناسبة لعملاء الخدمات السحابية، من قبيل المراقبة الذاتية لمستوى الخدمة والإشراف التلقائي للموارد المخصصة لهم.

7.2.2.7 اعتماد الشهادات الأمنية

ينبغي لمقدمي الخدمات السحابية أن يكونوا مسؤولين عن حيازة الشهادات الأمنية ذات الصلة، وينبغي أن يقوموا بتحديث هذه الشهادات بانتظام لتلبية متطلبات عملاء الخدمات السحابية.

وينبغي للمهندسين وغيرهم من موظفي هيئة مقدمي الخدمات السحابية أن يحضروا دورات التدريب الأمني وأن يكونوا مؤهلين للاضطلاع بعمليات منصات الحوسبة السحابية.

8.2.2.7 وثائق النشاط الأمني

يمكن لمقدمي الخدمات السحابية أن يقدموا الوثائق الأمنية التي تبين الجهود المبذولة لتعزيز أمن خدماتهم السحابية، من قبيل التدابير الأمنية المنفذة وإجراءات إدارة الأمن وما إلى ذلك. وينبغي الوصول إلى الوثائق بسهولة، مع إمكانية الاطلاع عليها أو تحميلها من موقع بوابتهم على شبكة الويب.

8 المبادئ التوجيهية المتعلقة بالأمن التشغيلي اليومي

ينبغي لمقدمي الخدمات السحابية أن ينفذوا التدابير الأمنية والأنشطة الأمنية للجهات الإدارية والمستأجرين في عملياتهم الأمنية اليومية. وينبغي تحقيق بند الأمن في اتفاق مستوى الخدمة وكفالته عن طريق التدابير والأنشطة الأمنية التي ينفذها مقدمو الخدمات السحابية. وتشمل هذه التدابير والأنشطة الأمنية، دون أن تقتصر على ذلك، ما يلي:

1) **التدابير الأمنية:** يطلب من مقدمي الخدمات السحابية تنفيذ مجموعة من التدابير الأمنية لتوفير القدرات والتسهيلات الأساسية من أجل تعزيز الأمن التشغيلي للحوسبة السحابية.
   - أ) تنص الفقرة 1.8 على إدارة الهوية ومراقبة النفاذ.
   - ب) تنص الفقرة 2.8 على تشفير البيانات وإدارة المفاتيح.
   - ج) تنص الفقرة 3.8 على الضوابط الأمنية للنظام.
   - د) تنص الفقرة 4.8 على التعافي من الأعطال الكبرى.
   - هـ) تنص الفقرة 5.8 على إدارة تشكيلة الأمن.
2) **الأنشطة الأمنية:** يطلب من مقدمي الخدمات السحابية القيام بالأنشطة الأمنية الروتينية لمعالجة المشاكل الأمنية وتأمين عملية الحوسبة السحابية.
   - أ) تنص الفقرة 6.8 على معالجة الأحداث الأمنية.

ب) تنص الفقرة 7.8 على تحديث البرمجيات التصحيحية.

ج) تنص الفقرة 8.8 على تأمين إدارة التشكيلة.

د) تنص الفقرة 9.8 على مواجهة حالات الطوارئ.

هـ) تنص الفقرة 10.8 على النسخ الاحتياطي.

و) تنص الفقرة 11.8 على تدقيق الأمن الداخلي.

1.8 إدارة الهوية ومراقبة النفاذ

1.1.8 إدارة الهوية

ينبغي لمقدمي الخدمات السحابية أن يوفروا إدارة الهوية الموحدة للجهات الإدارية الداخلية والمستأجرين الخارجيين، مما قد يوفر البيانات الأولية للمراقبة الموحدة للنفاذ والترخيص والتدقيق.

1) ينبغي أن تدعم توحيد الهوية، التي يمكن أن تحقق تقاسم معلومات الحساب والتزامن بين التطبيقات السحابية المختلفة في المنطقة الموثوقة ذاتها.

2) ينبغي أن تدعم إدارة دورة حياة الهوية، التي تشمل المراقبة الكاملة لدورة حياة الهوية، مثل سجل الهوية وإسناد الدور والامتيازات وتبديل الامتيازات وحذف الهوية، وما إلى ذلك. بالإضافة إلى ذلك، ينبغي أن يحظى تسجيل الهوية وتبديلها بإجراءات الموافقة من جانب الجهات الإدارية.

3) تشمل سياسات إدارة الهوية سياسة تسمية حساب الهوية وسياسة تطبيق حساب الهوية، وما إلى ذلك. وينبغي أن تشمل مجموعة السياسات الأمنية هذه ما يلي:

- ينبغي أن يكون اسم حساب الهوية فريداً في المنطقة الموثوقة ذاتها.
- ينبغي إغلاق حساب الهوية عندما يستمر إدخال كلمات السر غير الصحيحة.
- ينبغي تعطيل حساب الهوية عندما تطول فترة عدم استخدامه.
- ينبغي حظر حساب الهوية عند محاولة تسجيل الدخول بشكل متكرر خلال فترة زمنية قصيرة للغاية.

4) في إطار إدارة موحدة لحساب المستخدم، ينبغي أن يكون الحساب مضبوطاً لكي يرتبط بأشخاص أو مستأجرين محددين. وينبغي التعرف على المستخدمين عن طريق الحساب الرئيسي، وينبغي أن يتمتع كل مستخدم (المسؤول أو المستأجر) بحساب رئيسي واحد فقط. ويمكن للحساب الرئيسي أن يستحدث حساباً فرعياً، ويمكن أن يتمتع الحساب الفرعي بالامتيازات المخولة لإدارة خلايا الشبكة ومخدمات قوعد البيانات ومخدمات التطبيقات، إلخ.

5) ينبغي أن يركز تدقيق الحساب الموحد في المقام الأول على تخصيص حساب الهوية والسلوك فيما يتعلق بتسجيل الدخول وعملية الخروج وفقاً لوحدات مراقبة النفاذ، الأمر الذي يمكن أن يساعد على كشف الحسابات غير القانونية والحسابات التي تجاوزت تاريخ الاستحقاق، وإماطة اللثام عن الحسابات ذات الترخيص الزائد والحسابات التي تفتقر إلى ترخيص، ومنع محاولات تسجيل الدخول باستخدام حسابات متروكة أو حسابات مزورة. وينبغي أن يعرض الأحداث الأمنية للحسابات على وحدة أو أنظمة التدقيق الأمني من أجل القيام بمجموعة أوسع من وظائف التدقيق، من قبيل كشف التسلل وتدقيق مراقبة الأعطال، وما إلى ذلك.

6) ينبغي أن تدعم إدارة كلمة سر المستخدم، التي تتضمن المجموعة الموحدة لسياسات كلمة سر المستخدم استناداً إلى السياسة الأمنية لمنصة الحيز السحابي، من قبيل خوارزميات التشفير وطول كلمة السر وتعقد كلمة السر ودورة تحديث كلمة السر. وينبغي أن تدعم أشكالاً مختلفة من كلمات السر، من قبيل كلمات السر البيانية وكلمات السر الصوتية وما إلى ذلك. بالإضافة إلى ذلك، ينبغي أن تدعم وظائف تزامن كلمة السر وإعادة تحديدها.

7) ينبغي أن توفر الخدمة الذاتية للمستأجرين في إدارة الحساب، بحيث يضطلع المستأجرون ببعض أعمال الإدارة بأنفسهم، مثل تبديل بعض خصائص المستخدمين البسيطة وتحديث كلمة السر، مما قد يخفف عبء الصيانة على موظفي الإدارة.

2.1.8 إدارة مراقبة النفاذ

ينبغي لمقدمي الخدمات السحابية أن ينشئوا نظاماً مركزياً موحداً للاستيقان والتخويل لتحسين أمن مراقبة النفاذ في التشغيل اليومي. وينبغي أن تسجل السجلات التشغيلية بشأن مراقبة النفاذ إلى أنظمة الحوسبة السحابية للتدقيق فيها في وقت لاحق.

1) ينبغي للاستيقان الموحد أن يدعم الوظائف التالية:

- دعم التسجيل الوحيد للدخول (SSO): ينبغي أن يدعم ضبط معلمات التسجيل الوحيد للدخول، من قبيل دورة التصفح القصوى ومدة الشغور القصوى ومدة التخزين المؤقت القصوى.
- دعم تكنولوجيا الاستيقان العامة، من قبيل الاستيقان من بروتوكول النفاذ الخفيف إلى الدليل (LDAP) والاستيقان من إصدار الشهادات الرقمية والاستيقان من الرموز والاستيقان البيومتري والاستيقان متعدد العوامل، وما إلى ذلك.
- توفير سجلات استيقان مفصلة. وتشمل تعرف هوية النظام والمستخدمين المسجلين للدخول ووقت التسجيل للدخول ووقت الخروج وتسجيل الدخول إلى عنوان بروتوكول الإنترنت (IP) ومطراف تسجيل الدخول وسجلات نتائج الدخول (النجاح أو الفشل).
- توفير أساليب استيقان متمايزة واختيارية وفقاً لمختلف الأنظمة والخدمات. ويمكن أن تحقق التوازن بين مستوى الأمان وسهولة الاستخدام، بل والكلفة.

2) ينبغي للتخويل الموحّد أن يدعم الوظائف التالية:

- منح تخويل للنفاذ إلى الموارد السحابية، وفقاً للتحديد المسبق للمستخدمين وفئات المستخدمين ومستوى الامتيازات المخولة للمستخدمين.
- دعم آليات التخويل المركزي والتخويل الهرمي، وينبغي لمسؤول التخويل أن يقيد مجموعة التخويلات المتعلقة بالجهات الإدارية الهرمية المخولة.
- دعم سياسة التخويل عالية الدقة وسياسات التخويل المقسمة إلى أجزاء كبيرة.
- توفير سجلات استيقان مفصلة، بما فيها عناوين بروتوكول الإنترنت والمشغل ووقت التخويل، فضلاً عن التصاريح الممنوحة والملغاة.

3) المتطلبات الأخرى

- مراقبة النفاذ إلى السجلات. ينبغي لمقدمي الخدمات السحابية أن يضمنوا أنه في حالة نفاذ الجهات الإدارية إلى السجلات، فإنها تتمتع بالامتيازات الممنوحة لفعل ذلك. وينبغي أن يتمتع المستأجرون بالامتيازات التي تمنحها الجهات الإدارية لمعاينة السجلات المتعلقة بهم على نحو مناسب من خلال موقع إلكتروني لبوابة الخدمة الذاتية أو أدوات أخرى خاصة بالعملاء.
- آليات التشفير. ينبغي تشفير البيانات الحساسة، من قبيل بيانات الاستيقان وبيانات التخويل، وما إلى ذلك، في إجراءات التخزين والإرسال.
- ينبغي أن تكون جميع السجلات التشغيلية المتعلقة بعميل الخدمات السحابية مرئية على نحو مناسب.

2.8 تشفير البيانات وإدارة المفاتيح

يعتبر تشفير البيانات وإدارة المفاتيح الآليات الرئيسية لحماية البيانات في أنظمة الحوسبة السحابية. ويتيح تشفير البيانات القدرة على حماية الموارد، في حين تتيح إدارة المفاتيح مراقبة المفاتيح المشفرة التي تُستخدم لحماية الموارد.

وينبغي تحديد التنفيذ المعين لعملية التشفير بوضوح في بند الأمن في اتفاق مستوى الخدمة. بالإضافة إلى ذلك، ينبغي أن تمتثل عملية التشفير للمعايير الصناعية والحكومية ذات الصلة. ويبغي لمقدمي الخدمات السحابية أو عملاء الخدمات السحابية أن ينظروا بجدية في العناصر التالية:

1) تشفير إرسال البيانات في الشبكة. ومن الأهمية بصفة خاصة تأمين أوراق الاعتماد، من قبيل المعلومات المالية وكلمات السر، إلخ.
2) تشفير البيانات السكونية على القرص أو في قاعدة البيانات. ويمكن استخدامها لصد عملاء الخدمات السحابية أو المستأجرين المجاورين ذوي النوايا السيئة.
3) تشفير البيانات في وسائط النسخ الاحتياطي. ويمكن استخدامها لمنع تسرب البيانات في حالة فقدان وسائط النسخ الاحتياطي أو تعرضها للسرقة.

وإذا كان مقدم الخدمات السحابية هو المنفّذ الرئيسي لعملية تشفير البيانات، فإن إدارة المفاتيح مسألة أساسية خلال عمليات التشغيل اليومية. وينبغي لمقدم الخدمات السحابية أن يحدد إدارة مفاتيح متكاملة وينفذها في دورة الحياة التي تشمل عملية الإنشاء والاستخدام والتخزين والنسخ الاحتياطي والاستعادة والتحديث والإتلاف. وينبغي لمقدمي الخدمات السحابية أن ينظروا أيضاً في المسائل التالية:

1) حماية تخزين المفاتيح: يجب حماية تخزين المفاتيح مثلها مثل أي بيانات حساسة أخرى، بل ويجب أن يكون مستوى أمنها أعلى من مستوى أمن غيرها من البيانات. ولا يُسمح إلا لكيان محدد بالنفاذ إلى مكان تخزين المفاتيح. وثمة حاجة أيضاً إلى وضع سياسات ذات صلة مثل فصل الأدوار لفرض مراقبة أشد على عملية النفاذ.
2) النسخ الاحتياطي والاستعادة: نظراً إلى أن أي خسارة غير متوقعة لمفتاح محدد يمكن أن تلحق الضرر بالخدمة، فمن الضروري تنفيذ نسخة احتياطية للمفاتيح وحل للاستعادة.
3) إدخال الطرف الثالث لإدارة المفاتيح: عن طريق مجموعة من عمليات فصل بين المهام، يمكن أن يساعد مقدمي الخدمات السحابية على تجنب التعارض مع المتطلبات القانونية عندما يُزعم توفير البيانات في أنظمة الحوسبة السحابية.

3.8 مراقبة أمن النظام

أثناء عمليات التشغيل اليومية، ينبغي لمقدمي الخدمات السحابية أن ينفذوا مراقبة أمنية مركزية في الوقت الفعلي بشأن منصة الحيز السحابي وبنيته التحتية، بحيث تشمل حالة تشغيل مختلف الموارد المادية والافتراضية. ومن خلال النظر في الشروط الرئيسية لاتفاق مستوى الخدمة (من قبيل أداء الشبكة واستخدام الموارد الرئيسية والتخزين، إلخ.)، وتحليل جميع أنواع السجلات، يمكن لمقدمي الخدمات السحابية أن يضطلعوا بإدارة الأعطال، وإدارة الأداء، وإدارة التفتيش التلقائي لتحقيق الهدف المتمثل في مراقبة الحالة الصحية للموارد السحابية في الوقت الفعلي أو في الوقت شبه الفعلي.

وبوجه عام، يتولى مقدمو الخدمات السحابية إدارة سجلات المراقبة وحمايتها بصرامة. ومع ذلك، بمجرد أن يكون عملاء الخدمات السحابية بحاجة إليها، يمكن لمقدمي الخدمات السحابية أن يزودوهم بسجلات المراقبة ذات الصلة كما طالبوا بها، وعلى سبيل المثال، قد يحتاج عملاء الخدمات السحابية إلى سجلات المراقبة ذات الصلة لحل المشكلات القائمة في مواجهة حالات الطوارئ.

كما يمكن لمقدمي الخدمات السحابية أن يقوموا بالكشف الاستباقي للمخاطر التشغيلية المحتملة وحلها في الوقت المناسب. بالإضافة إلى ذلك، ينبغي لمقدمي الخدمات السحابية أن يوفروا القدرة اللازمة لتحليل الترابط بين عملاء الخدمات السحابية وخدماتهم التي يوفرها مقدمو الخدمات السحابية، والتي يمكن تنفيذها لتشخيص حالة الخدمات السحابية من حيث النوعية والأمن.

وهناك نوعان من أساليب الضوابط الأمنية: المراقبة التلقائية والتفتيش اليدوي، اللذان يعتمدان على الوسائل والإدارة التقنية لفرادى مقدمي الخدمات السحابية. ويتضمن موضوع الضوابط الأمنية ما يلي:

1) مراقبة الحالة الصحية للبنية التحتية للحوسبة السحابية: ينبغي لمقدمي الخدمات السحابية أن يوفروا القدرة اللازمة لجمع ومراقبة سجلات الأحداث الأمنية والمعلومات المتعلقة بمواطن الضعف وتبديل تشكيلة الأجهزة الأمنية والوضع الأدائي والتشغيلي بشأن جميع مجالات البنية التحتية للحوسبة السحابية، التي تشمل موارد الآلة الافتراضية (VM) ومنصة إدارة الحوسبة السحابية والأجهزة الأمنية وقاعدة البيانات، وما إلى ذلك. ويمكن لهذه المراقبة أن تساعد مقدمي الخدمات السحابية على الإبقاء على وعي مميز بالحالة الصحية الشاملة والحالة التشغيلية للبنية التحتية للحيز السحابي.

2) الكشف عن السلوك الشاذ: يتضمن السلوك الشاذ تسجيل الدخول غير القانوني والنفاذ غير القانوني إلى منصة إدارة الحيز السحابي والنفاذ المنتهك للموارد الأخرى والتعديلات الشاذة المدخلة على تشكيلات معدات الشبكة والآلات الافتراضية أو الهجمات المخترقة الأخرى، التي يمكن تنفيذها باستخدام الوسائل التقنية، مثل أدوات التدقيق المتكاملة أو برمجيات منع تسرّب البيانات (DLP) أو الأدوات الأمنية الأخرى.

3) مراقبة الحركة الشاذة في الشبكة: ينبغي أن يتمتع مقدمو الخدمات السحابية بالقدرة على كشف وتحليل الحركة الشاذة في الشبكة المادية والشبكة الافتراضية، لا سيما الحركة داخل الآلات الافتراضية. ومن الضروري الإبقاء على الوعي بالحركة الشبكية والوضع الأدائي، الأمر الذي قد يساعد مقدمي الخدمات السحابية على تحسين القدرة الدفاعية ضد الديدان الحاسوبية وهجمات الحركة الشاذة وغيرها من التهديدات الأمنية المحتملة في بيئة الحوسبة السحابية.

4) مراقبة الأمن المادي: تتضمن مجالات مراقبة الأمن المادي نظام مراقبة درجة الحرارة والرطوبة والدوائر التلفزيونية المغلقة (CCTV) وحارس المدخل ونظام الحماية من الحرائق ومكيف الهواء ونظام الإمداد بالطاقة والمراقبة والأقفاص الوقائية، إلخ.، التي يمكن تفقدها يومياً.

والأهم من ذلك كله، ينبغي أن يجري مقدمو الخدمات السحابية مجموعة كاملة من المراجعات لبيئة الحوسبة السحابية للحصول على الحالة الصحية لخدمات الحوسبة السحابية أثناء التشغيل والصيانة اليوميين. ومن شأن ذلك أن يساعد مقدمي الخدمات السحابية على الكشف السريع عن مختلف المؤشرات، من قبيل نوعية أداء الشبكة وأداء الآلات الافتراضية ونوعية الخدمات الموجهة نحو عملاء الخدمات السحابية وما إلى ذلك. بالإضافة إلى ذلك، يمكن تكييف عملية الفحص لدعم العتبة، بل وحتى إنذار قيمة خط الأساس. واستناداً إلى معلومات المراقبة المجمعة، ينبغي أن يكون مقدمو الخدمات السحابية قادرين على الوصول بسرعة إلى مصدر المشاكل في الشبكة والتخزين والآلات المادية والمنصات الافتراضية عند حدوث أي عطل.

وينبغي أن يتمتع مقدمو الخدمات السحابية أيضاً بالقدرة على تحديد موقع عملاء الخدمات السحابية الذين يُحتمل أن يتأثروا من خلال إجراء تحليل للترابط بشأن كل عطل بعينه، استناداً إلى الافتراض بأن لدى عملاء الخدمات السحابية نفس مواطن الضعف والتطبيقات والنسخة المحددة لنظام التشغيل، إلخ.

4.8 التعافي من الأعطال الكبرى

ينبغي لمقدمي الخدمات السحابية أن ينفذوا التدابير الأمنية المتعلقة بالتعافي من الأعطال الكبرى بحيث تحقق مستوى الأمن ذاته الذي تحققه الأنظمة الأولية. وتشمل تكنولوجيا التدابير الأمنية مجموعات المخدّمات والاستنساخ المتزامن عن بُعد والاستنساخ غير المتزامن عن بُعد لتوفير طاقة بديلة فورية للتعافي من الأعطال الكبرى.

1) حشد المخدمات

يمكن لعملية حشد المخدمات أن تنسق وتدير أخطاء وأعطال المكونات المنفصلة، ويمكنها أن تضيف مكونات إلى المجموعة بشفافية، مع المرونة والقدرة على التوسع لتحقيق الأداء الكافي.

2) الاستنساخ المتزامن عن بُعد

من خلال برمجيات الاستنساخ المتزامن عن بُعد، يتم نسخ البيانات بصورة متزامنة من الموقع الرئيسي وإرسالها إلى موقع بعيد. وبمجرد أن يتعطل الموقع الرئيسي، فإن البرامج الجاري تشغيلها تتحول إلى الموقع البعيد. ويمكن للاستنساخ المتزامن عن بُعد أن يضمن استمرار الأعمال دون فقدان البيانات. وتكلفة هذا الأسلوب مرتفعة لأنها تعتمد على برمجيات استنساخ مصممة بدقة وعرض نطاق كاف على الشبكة. ويجري تنفيذ الاستنساخ المتزامن عن بُعد بانتظام في أنظمة تتمتع بمستوى أمني عال.

3) الاستنساخ غير المتزامن عن بُعد

وهو أسلوب آخر للاستنساخ عن بُعد، حيث تقل عادة تكلفته عن تكلفة الاستنساخ المتزامن عن بُعد. ويتم استنساخ بيانات الموقع الرئيسي على نحو دوري وإرسالها إلى موقع بعيد. وإذا كانت الأمور تسير على ما يرام، فإن باستطاعة هذا الاستنساخ أن يضمن توفير نسخة كاملة في الموقع البعيد دون خفض مستوى أداء الموقع الرئيسي. ولكن إذا حدث خطأ ما خلال فترة الاستنساخ، فإن فقدان البيانات يصبح أمراً محتوماً. ويمكن اختيار الاستنساخ غير المتزامن عن بُعد عقب تقييم كاف للمخاطر.

5.8 إدارة تشكيلة الأمن

تشمل تشكيلة الأمن قواعد الأمن المشكلة في المنصة السحابية والشبكة والآلات الافتراضية والمكونات المختلفة للتطبيقات. وهي تختلف عن السياسة الأمنية رفيعة المستوى، التي تحدد نهج المنظمة لتحقيق أهداف أمن المعلومات.

وينبغي لمقدمي الخدمات السحابية أن يضطلعوا بإدارة تشكيلة الأمن المتكاملة لتوفير التنفيذ الفعال والنشر السريع لتشكيلة الأمن.

ويُقترح أن يقوم مقدمو الخدمات السحابية، في إطار إدارة تشكيلة الأمن، بتحديد نماذج معيارية لتشكيلة السياسة الأمنية وسياسة أساسية لتشكيلة الأمن. بالإضافة إلى ذلك، ينبغي لمقدمي الخدمات السحابية أن يتخذوا التدابير اللازمة لضمان اتساق تشكيلة الأمن وكفاءتها عندما تتغير البيئة السحابية، ولإفراد تشكيلة الأمن فيما بين عملاء الخدمات السحابية في بيئة متعددة الشاغلين.

وتشمل النماذج المعيارية لتشكيلة الأمن النماذج المعيارية الرئيسية لتشكيلة الأمن، التي تتطلبها بيئة الحوسبة السحابية الحالية، من قبيل إدارة الحسابات والاستيقان وسياسات مراقبة النفاذ وسياسات التدقيق وسياسات الاستجابة الدينامية وسياسات تحديث التطبيقات والبرمجيات وسياسات النسخ الاحتياطي والاستعادة، إلخ.

وتوفر التشكيلة الأساسية للأمن معياراً لمتطلبات تشكيلة الأمن فيما يتعلق ببيئة الحوسبة السحابية بكاملها، الأمر الذي قد يساعد مقدمي الخدمات السحابية على تقييم ما إذا كانت تشكيلة الأمن الحالية تستجيب لمستوى الأمن الأساسي أم لا، وكذلك توفير إرشادات مفصلة لتعزيزها. وينبغي أن تشمل فئات التشكيلة الأساسية للأمن، دون أن تقتصر على ذلك، ما يلي: التشكيلة الأساسية لأمن نظام التشغيل والتشكيلة الأساسية لأمن قاعدة البيانات والتشكيلة الأساسية لأمن جدار الحماية والتشكيلة الأساسية لأمن التحول والتشكيلة الأساسية لأمن المسيّرات، إلخ.

وتتضمن إدارة تشكيلة الأمن التدابير التالية:

1) إدارة النموذج المعياري لتشكيلة الأمن

ينبغي لمقدمي الخدمات السحابية أن يحددوا النماذج المعيارية الرئيسية للأمن لتلبية متطلبات البيئة السحابية اللازمة لجعل عملية نشر تشكيلة الأمن أسرع وأنسب. وينبغي لإدارة النموذج المعياري لتشكيلة الأمن أن تدعم النماذج المعيارية المكيفة، وأن تتولى تحديث النماذج المعيارية وتحقيق استخدامها الأمثل على نحو مستمر حسب تغيرات المنصة السحابية ووضع الشبكة ومتطلبات الخدمة وما إلى ذلك.

علاوةً على ذلك، ينبغي لمقدمي الخدمات السحابية أن يزودوا عملاء الخدمات السحابية بالكفاءة اللازمة لتكييف النماذج المعيارية الجديدة لتشكيلة الأمن وفقاً لاحتياجاتهم الخاصة. بالإضافة إلى ذلك، ينبغي أن يكون عملاء الخدمات السحابية مسؤولين عن فعالية تشكيلة الأمن التي تولوا تكييفها.

2) إدارة عملية تشكيلة الأمن

ينبغي أن يبرهن مقدمو الخدمات السحابية على فعالية تشكيلة الأمن. ويمكن تشكيل تشكيلة الأمن وفقاً لمتطلبات عملاء الخدمات السحابية والخدمات السحابية. وتضم العملية الرئيسية لإدارة تشكيلة الأمن طلب التشكيلة والموافقة على التشكيلة والاختبارات والإقرار التقني والتنفيذ وحفظ التشكيلة وتقرير النتائج.

3) إدارة التشكيلة الأساسية للأمن

ينبغي أن يطور مقدمو الخدمات السحابية التشكيلة الأساسية للأمن من خلال النظر بشكل شامل في المتطلبات الأمنية لمنصة الحوسبة السحابية والخدمات السحابية وعملاء الخدمات السحابية وبند الأمن في اتفاق مستوى الخدمة وما إلى ذلك.

وتتضمن العملية الرئيسية لإدارة التشكيلة الأساسية للأمن طلب وسجل التحقق من تشكيلة الأمن والموافقة والتحقق من التنفيذ والتحقق من نتائج التقرير وتنفيذ إجراءات التعزيز ونتائج تقرير إجراءات التعزيز. وينبغي إجراء عملية التحقق من تشكيلة الأمن على نحو دوري خلال عمليات التشغيل اليومية، ويمكن تنفيذها عن طريق جمع التشكيلات وتحليل الأمن الأساسي.

4) إدارة تعارض تشكيلة الأمن

في بيئة سحابية لتقاسم الموارد، وبسبب الأعطال الناجمة عن الجهات الإدارية المسؤولة عن الأمن أو عن أسباب أخرى، يمكن المساس بتشكيلة الأمن مما قد يؤدي إلى ظهور مواطن ضعف في بيئة الحوسبة السحابية. وينبغي أن ينفذ مقدمو الخدمات السحابية تدابير فعّالة لكشف أوجه تعارض تشكيلة الأمن، واستحداث عملية لمعالجتها وآليات للاستعادة.

وينبغي أن تتضمن عملية معالجة تعارض تشكيلة الأمن نظام إنذار في حالة حدوث تعارض وتحليل التعارض (وهو يضم تحليل الأسباب والتأثيرات) ومعالجة التعارض وتقرير النتائج.

5) إدارة انتقال تشكيلة الأمن

عندما تتغير موارد أو خدمات الحوسبة السحابية (مثل توسيع نطاق القدرة على تقديم الخدمات والآلات الافتراضية وما إلى ذلك)، ينبغي أن يوفر مقدمو الخدمات السحابية وسائل دينامية لتعديل تشكيلة الأمن. وعلى سبيل المثال، أثناء انتقال الآلات الافتراضية، يمكن تنفيذ الانتقال التلقائي لسياسة تشكيلة الأمن من خلال استشعار حالة الانتقال والمواءمة التلقائية وإعادة نشر السياسة الأولية لتشكيلة الأمن، الأمر الذي يمكن أن يكفل الاتساق في سياسة تشكيلة الأمن والنشر السريع في البيئة السحابية، وأن يحسن كفاءة العمليات الأمنية.

6) إدارة إفراد تشكيلة الأمن

في بيئة متعددة الشاغلين للحوسبة السحابية، ينبغي أن يضطلع مقدمو الخدمات السحابية بإدارة تصنيف صارمة لتشكيلة أمن عملاء الخدمات السحابية، وأن يتخذوا التدابير اللازمة مثل الاستيقان ومراقبة النفاذ وما إلى ذلك. وذلك في سبيل ضمان إفراد تشكيلة الأمن فيما بين مختلف عملاء الخدمات السحابية.

6.8 معالجة الأحداث الأمنية

ينبغي أن يضطلع مقدمو الخدمات السحابية ببعض الأنشطة لمعالجة الأحداث الأمنية في بيئة الحوسبة السحابية، من قبيل الإنذار بالتهديد والتبليغ عن مواطن الضعف ومواجهة حالات الطوارئ، إلخ. كما ينبغي أن يعمم مقدمو الخدمات السحابية تدابير تقنية للمساعدة على كشف الأحداث الأمنية والتنبيه إليها ومعالجتها.

وبوجه عام، تتضمن إجراءات معالجة الأحداث الأمنية في بيئة الحوسبة السحابية الخطوات التالية: الكشف عنها وتحليلها والتخلص منها والتحقق منها والتبليغ عنها وتسجيلها. وينبغي لمقدمي الخدمات السحابية أن يحددوا بوضوح الأشخاص المسؤولين عن كل خطوة من هذه الخطوات.

1.6.8 الكشف عنها

ينبغي أن يتخذ مقدمو الخدمات السحابية التدابير اللازمة لمراقبة الوضع الأمني للمنصة السحابية الواردة في الفقرة 3.8، وأن تكون لديهم القدرة على إرسال الإنذارات في الوقت المناسب كلما وقعت أحداث أمنية. وينبغي لهم ضمان أن يُوجه الإنذار إلى الشخص المحدد، مثل مدير أمن منصة الحوسبة السحابية. ويمكن إرسال الإنذارات عن طريق البريد الإلكتروني، أو المكالمات الهاتفية، أو خدمة الرسائل القصيرة (SMS)، إلخ. وينبغي أن يتأكد مقدمو الخدمات السحابية من مراقبة جميع أنواع الأحداث الأمنية المنصوص عليها في بند الأمن في اتفاق مستوى الخدمة.

2.6.8 تحليلها

ينبغي أن يؤكد مقدمو الخدمات السحابية الأحداث الأمنية بعد تلقي الإنذارات، ثم تحليلها وتشخيصها لتحديد أنواع الأحداث وأسبابها والتدابير التي يتعين اتخاذها لمعالجتها. ويمكن لمقدمي الخدمات السحابية أن يتصلوا بعملاء الخدمات السحابية من أجل تقديم المساعدة، عند اللزوم.

3.6.8 التخلص منها

ينبغي أن يتخذ مقدمو الخدمات السحابية تدابير علاجية وفقاً لأنواع ومستويات الأحداث الأمنية، من أجل التقليل إلى الحد الأدنى من آثارها. وينبغي أن يرجع مقدمو الخدمات السحابية إلى الأنشطة الأمنية الواردة في الفقرات 7.8 و8.8 و9.8، التي تشمل، دون أن تقتصر على ذلك، ما يلي:

1) في حالة وقوع طارئ أمني، ينبغي أن يتخذ مقدمو الخدمات السحابية التدابير اللازمة وفقاً لخطط مواجهة حالات الطوارئ.
2) في حالة حدوث ثغرة أمنية، ينبغي أن يتخذ مقدمو الخدمات السحابية الإجراءات اللازمة وفقاً لتحديث البرمجيات التصحيحية.
3) في حالة بروز موطن ضعف على التشكيلة، ينبغي أن يتخذ مقدمو الخدمات السحابية الإجراءات اللازمة وفقاً لتأمين إدارة التشكيلة.

وينبغي أن يضطلع مقدمو الخدمات السحابية بمراقبة الأحداث الأمنية وتقييمها على نحو دينامي، وإطلاع عملاء الخدمات السحابية على المعلومات ذات الصلة والتقدم المحرز فيما يتعلق بمعالجتها.

4.6.8 التحقق منها

بعد التخلص من الأحداث الأمنية، ينبغي أن يواصل مقدمو الخدمات السحابية تحليل الأسباب والحالات التي قد تتسبب في حدوثها، والتحقق مما إذا كان لدى عملاء الخدمات السحابية نظام آخر يعاني من مواطن الضعف ذاتها التي يمكن أن تتسبب في الأحداث الأمنية نفسها. وإذا ثبت وجود مواطن ضعف، فينبغي لمقدمي الخدمات السحابية أن يخطروا عملاء الخدمات السحابية المعنيين فوراً وأن يتخذوا الإجراءات المقابلة. وينبغي ألا ينطوي الإخطار على أي خصوصيات تتعلق بعملاء آخرين للخدمات السحابية.

5.6.8 التبليغ عنها وتسجيلها

ينبغي أن يعد مقدمو الخدمات السحابية تقريراً بشأن معالجة الأحداث الأمنية يتضمن سلوك الأحداث الأمنية وأسبابها والتدابير المتخذة لمعالجتها، وما إلى ذلك، وأن يتولوا إرساله إلى عملاء الخدمات السحابية المعنيين خلال المهلة المحددة في بند الأمن في اتفاق مستوى الخدمة. وينبغي أن يسجل مقدمو الخدمات السحابية المعلومات المتعلقة بالأحداث الأمنية لكي تستفيد منها عملية التفتيش والتدقيق اللاحقة. ويمكن تقديم التقارير المناسبة إلى عملاء الخدمة السحابية المتأثرين وإلى المراجعين المعتمدين من أطراف ثالثة (الذين يقومون بدور الشريك في الخدمة السحابية).

7.8 تحديث البرمجيات التصحيحية

1.7.8 المسؤوليات

ينبغي لمقدمي الخدمات السحابية أن يحققوا الاستخدام الأمثل لعملية إدارة البرمجيات التصحيحية بشأن المنصة السحابية للحد من المخاطر المحتملة الناجمة عن مواطن الضعف القائمة، وأن يتولوا حماية التشغيل المستقر للمنصات والخدمات السحابية.

وينبغي تنفيذ إدارة البرمجيات التصحيحية، في إطار الحوسبة السحابية، على نحو مشترك بين مقدمي الخدمات السحابية وعملاء الخدمات السحابية.

1) مسؤوليات مقدمي الخدمات السحابية:

- تتبع بيانات مواطن ضعف أنظمة تشغيل النسخ وإيجاد أحدث البرمجيات التصحيحية في الوقت المناسب؛
- اختبار أمن البرمجيات التصحيحية وقابليتها للتكيف؛
- تحديث البرمجيات التصحيحية لنظام تشغيل النسخ وخلق أحدث ملفات الصور؛
- إعلام عملاء الخدمات السحابية ومساعدتهم على إتمام تحديث البرمجيات التصحيحية، وضمان عدم بروز مواطن الضعف ذاتها في المستقبل؛
- تنفيذ اختبار تأثير أحدث ملفات الصور هذه من خلال استحداث آلة افتراضية جديدة.

2) مسؤوليات عملاء الخدمات السحابية:

- مساعدة مقدمي الخدمات السحابية على تتبع بيانات مواطن الضعف وإيجاد أحدث البرمجيات التصحيحية؛
- تحديث البرمجيات التصحيحية للآلة الافتراضية في الوقت المناسب وفقاً للمعلومات الواردة من مقدمي الخدمات السحابية.

ووفقاً لأسلوب خدمة الحوسبة السحابية، من قبيل البنية التحتية كخدمة والمنصات كخدمة والبرمجيات كخدمة، يكون مقدمو الخدمات السحابية مسؤولين فقط عن الموارد التي يتحكمون فيها بمفردهم، وينسحب ذلك على عملاء الخدمات السحابية. وفيما يتعلق بالبنية التحتية كخدمة، ينبغي أن يكون مقدمو الخدمات السحابية مسؤولين عن تحديث البرمجيات التصحيحية للبنية التحتية للحوسبة السحابية، ويكون عملاء الخدمات السحابية مسؤولين عن نظام التشغيل الخاص بالضيوف وبرمجيات التطبيق وما إلى ذلك، التي يتحكم فيها عملاء الخدمات السحابية.

2.7.8 عملية تحديث برمجية الأمن التصحيحية

تضم مكونات المنصة السحابية التي تحتاج إلى البرمجيات التصحيحية برمجيات التمثيل الافتراضي وأنظمة التشغيل ومعدات الشبكة والمعدات الأمنية ومخدمات قواعد البيانات ومطاريف الإدارة وغيرها من مكونات المنصة السحابية. وتتضمن عملية العروة المغلقة لتحديث البرمجيات التصحيحية أربع مراحل كما هو موضح أدناه، الأمر الذي يمكن أن يساعد مقدمي الخدمات السحابية على ضمان أفضل الآجال فيما يتعلق بإصلاح منصتهم السحابية.

1) جمع البرمجيات التصحيحية

ينبغي أن يجمع مقدمو الخدمات السحابية المعلومات عن البرمجيات التصحيحية من الموقع الرسمي لتحديث البرمجيات التصحيحية الخاص بالجهات البائعة، وأن يستخدموا الأدوات التلقائية لتحديث البرمجيات التصحيحية التي تصدرها الجهات البائعة، أو من خلال وسائل أخرى لضمان نزاهة متطلبات البرمجيات التصحيحية. وينبغي أن يقوم مقدمو الخدمات السحابية بإجراء تحليل للبرمجيات التصحيحية المجمعة، والبحث عن مواطن ضعف الأنظمة والتطبيقات القائمة وتسجيلها، وتقييم الآثار والمخاطر المحتملة لعملية الإصلاح، وتحديد مدى الحاجة الماسة إلى البرمجيات التصحيحية وأهميتها.

2) اختبار البرمجيات التصحيحية

ينبغي أن يبدأ مقدمو الخدمات السحابية بإجراء اختبار للبرمجيات التصحيحية للتحقق من أمنها واتساقها واستقرارها. وينبغي أن يهيئوا بيئة لإجراء اختبار لمضاهاة المنصة أو الأنظمة المستهدفة قبل استهلال مرحلة الإصلاح. وبعد إجراء الاختبار، ينبغي إعداد تقرير يمكن أن يقترح ما إذا كان من الضروري طرح برمجيات التصحيح أم لا. كما يقدم تقرير الاختبار مبادئ توجيهية تقنية مفصلة بشأن خطوات الإصلاح وبرنامج استئناف المعالجة. وينبغي أن يقدم وصفاً كاملاً للبرمجيات التصحيحية لمساعدة مهندسي الإصلاح على الإحاطة بوظائف هذه البرمجيات وعملياتها، وآثارها على الأنظمة والتطبيقات، مثل المشاكل الناتجة عن البرمجيات التصحيحية والأنظمة المتأثرة، وما إذا كان من الضروري إعادة تحميل النظام أو التطبيق أم لا، وما إلى ذلك.

3) تحديث البرمجيات التصحيحية

ينبغي أن يعد مقدمو الخدمات السحابية خطة تشغيلية لتحديث البرمجيات التصحيحية تشمل الخطوات التشغيلية المفصلة وفقاً لتقرير اختبار هذه البرمجيات. وينبغي أيضاً وضع خطة للطوارئ تشمل تخزين نسخ احتياطية للنظام والبيانات وتبديل التطبيقات ومراقبة توقيت طرح البرامج التصحيحية وإلغاء تثبيتها واستئناف معالجة النظام، في حالة حدوث عطل في البرمجيات التصحيحية. وبالنسبة إلى طرح البرمجيات التصحيحية على نطاق واسع، ينبغي لمقدمي الخدمات السحابية أن يطالبوا الجهات البائعة مسبقاً بتقديم الدعم التقني لتحسين القدرة على معالجة حالة الطوارئ في الحالات غير المتوقعة.

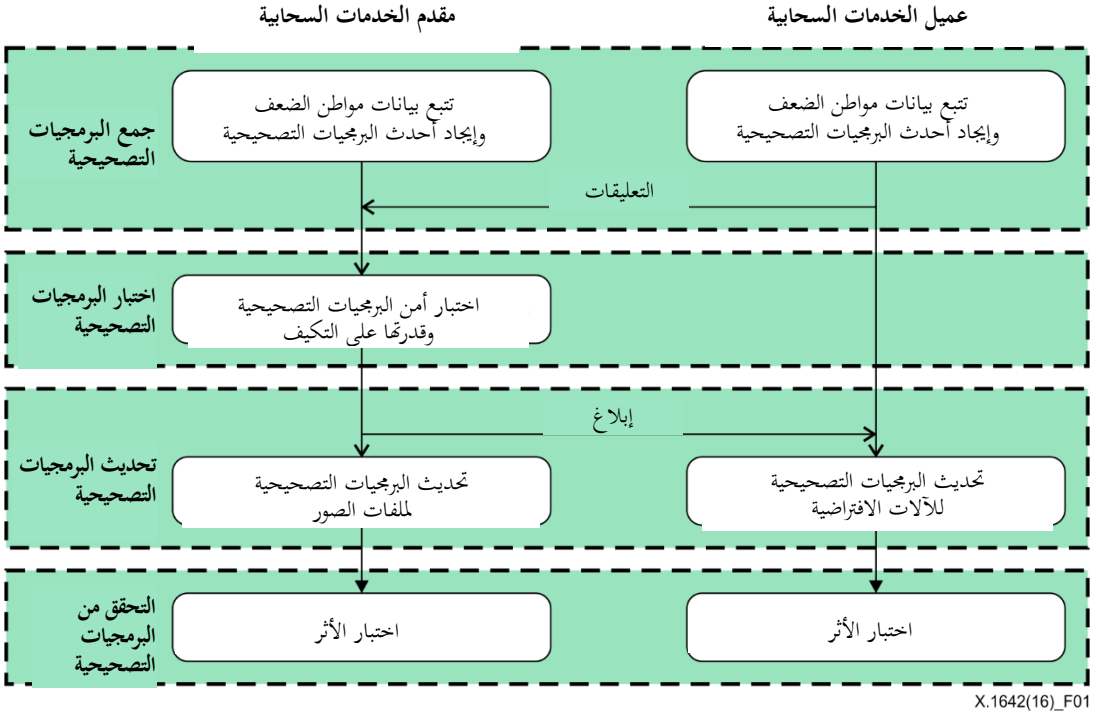
وينبغي أن يتمتع مقدمو الخدمات السحابية بالشفافية إزاء عملاء الخدمات السحابية عند طرح البرمجيات التصحيحية على المنصة السحابية، وينبغي أن يتواصلوا بوضوح مع هؤلاء العملاء قبل بدء الإصلاح. وينبغي ألا يحاول مقدمو الخدمات السحابية التأثير بأي شكل من الأشكال في خدمات عملاء الخدمات السحابية، وذلك من خلال اعتماد تدابير مناسبة بالتعاون مع هؤلاء العملاء.

4) التحقق من البرمجيات التصحيحية

بعد طرح البرمجيات التصحيحية، ينبغي لمقدمي الخدمات السحابية أن يتحققوا بانتظام من هذه البرمجيات باستخدام أدوات إدارة البرمجيات التصحيحية للتأكد من أن المنصة السحابية بكاملها تحتوي على أحدث البرمجيات التصحيحية. وينبغي تحديث وثيقة سجلات الإصلاح على نحو منتظم وينبغي حفظها لكي يستفيد منها التدقيق الأمني في وقت لاحق.

وينبغي أن يكون وقت الانتظار الذي يفصل بين جمع البرمجيات التصحيحية وتحديثها وشرط موافقة عملاء الخدمات السحابية على تحديث هذه البرمجيات واضحاً في اتفاق مستوى الخدمة، استناداً إلى صنف الأولوية التي تحظى بها البرمجيات التصحيحية (مثل حرجة وعالية ومتوسطة ومتدنية).

وفيما يلي مثال على عملية تحديث البرمجيات التصحيحية للأمن، بما فيها تحديث الآلة الافتراضية وملفات الصور الخاصة بها. وخلال هذه العملية، وفي حالة طرح أي برمجيات تصحيحية حديثة، سيضطلع مقدمو الخدمات السحابية باختبار أمنها وقابلية تكيفها. بالإضافة إلى ذلك، يتحمل عملاء الخدمات السحابية مسؤولية إيجاد أحدث البرمجيات التصحيحية وجمعها. وبعد إجراء اختبار ناجح لأحدث البرمجيات التصحيحية، سيتولى مقدمو الخدمات السحابية إعلام العملاء من أجل تحديث هذه البرمجيات. وفي الوقت نفسه، سيقوم مقدمو الخدمات السحابية بتحديث البرمجيات التصحيحية لملفات الصور الحالية. ويمكن بعد ذلك لمقدمي الخدمات السحابية استحداث آلة افتراضية جديدة بملفات الصور الجديدة هذه. وسينفذ أيضاً مقدمو الخدمات السحابية مسحاً محدداً للتأكد من أن عملاء الخدمات السحابية قد نجحوا في تحديث هذه البرمجيات.



الشكل 1- مثال لعملية تحديث البرامج التصحيحية للأمن

8.8 تأمين إدارة التشكيلة

ينبغي أن ينفذ مقدمو الخدمات السحابية الضوابط الأمنية لإدارة تشكيلة المنصة السحابية وتشكيلة الشبكة ومعلمات مختلف مكونات التطبيقات، الأمر الذي يمكن أن يساعد على الحد من المخاطر التشغيلية الناجمة عن أخطاء التشكيل أو سوء الاستخدام، ويعزز أمن بيئة الحوسبة السحابية واستقرارها.

وعادة ما تشمل إدارة التشكيلة إدارة تعديل التشكيلة وإدارة طرحها. وينبغي أن يتخذ مقدمو الخدمات السحابية التدابير اللازمة للتأكد من مراقبة وتسجيل تعديل التشكيلة وطرحها. وتيسيراً لإدارة التشكيلة، يجري في العادة وضع قاعدة بيانات متكاملة لإدارة التشكيلة، بحيث تضم السجلات الحالية والسجلات التاريخية لجميع ملفات التشكيلة والسياسة الأمنية والبيانات الوصفية لتطبيق كل عنصر ومكون للحوسبة السحابية. وينبغي أن يوفر مقدمو الخدمات السحابية الحماية لقاعدة البيانات هذه من النفاذ غير المرخص لها وتسرب المعلومات وما إلى ذلك.

ويتضمن أمن إدارة التشكيلة التدابير التالية:

1) تدقيق إدارة التشكيلة

الغرض من تدقيق إدارة التشكيلة هو ضمان تنفيذ متطلبات تعديل التشكيلة وطرحها بكفاءة وفعالية. ويمكن أن تساعد مقدمي الخدمات السحابية على التحقق من صحة كل عنصر من عناصر التشكيلة واتساقه واكتماله وصلاحيته وإمكانية تتبعه.

وينبغي تنفيذ تدقيق إدارة التشكيلة على نحو دوري خلال العمليات التشغيلية اليومية. وينبغي تسجيل جميع سجلات نفاذ المستخدم وتعديلاتها ومحفوظاتها وعمليات استعادتها وحفظها لغرض التدقيق عبر شبكة الإنترنت أو خارجها.

إضافة إلى ذلك، ينبغي أن يكون تقرير تدقيق إدارة التشكيلة المتعلق بعملاء الخدمات السحابية أو خدماتهم جلياً كما ينبغي لهؤلاء العملاء لتمكينهم من الإشراف على التدابير الأمنية وفعالية مقدمي الخدمات السحابية.

2) مراقبة إدارة التشكيلة

ينبغي أن يتولى مقدمو الخدمات السحابية مراقبة جميع التعديلات المدخلة على ملفات تشكيلة بيئة الحوسبة السحابية بكاملها والعمليات الأخرى، لمنع النفاذ غير المرخص له والتسرب والتعديلات غير القانونية وأخطاء التشكيل.

3) حماية قاعدة بيانات إدارة التشكيلة

ينبغي أن يقوم مقدمو الخدمات السحابية على نحو دقيق بصيانة وإدارة قاعدة بيانات إدارة التشكيلة، من قبيل إسناد السلطة على أساس الأدوار وإزالة النفايات والتدقيق المنتظم وحفظ نسخ احتياطية على نحو دوري، إلخ.

9.8 خطط المواجهة في حالات الطوارئ

من الأهمية بمكان ضمان قدرة أنظمة الحوسبة السحابية على أن تستجيب لمقدمي الخدمات السحابية بفعالية دون انقطاع مفرط عقب حادث أمني. وتدعم خطة المواجهة في حالات الطوارئ هذا المطلب من خلال وضع برنامج فعّال واتخاذ إجراءات وتدابير تقنية.

وبغية الحد من تأثير الحوادث الأمنية على منصات الحوسبة السحابية وخدماتها، ينبغي لخطة مقدمي الخدمات السحابية بشأن مواجهة حالات الطوارئ أن تقدم توجيهات واضحة للمشغلين وأن تحقق توازناً بين مستوى التفاصيل ودرجة المرونة. ويمثل وضع خطة للمواجهة في حالات الطوارئ وإدارتها دورة من عملية تحسين مستمر تتكون من ثلاث مراحل: مرحلة وضع الخطة ومرحلة اختبارها وتنفيذها ومرحلة صيانتها.

1.9.8 مرحلة وضع الخطة

ينبغي، قبل كل شيء، اعتماد طرائق التحليل النوعي والكمي لإجراء تقييم شامل للمخاطر وتحليل التأثير التجاري (BIA) لأنظمة الحوسبة السحابية. وبعد ذلك، يمكن الحصول على السمات الرئيسية للنظام ومكوناته، فضلاً عن أثر الحوادث الأمنية المختلفة. وعلى هذا الأساس، ووفقاً لبند الأمن في اتفاق مستوى الخدمة بين مقدمي الخدمات السحابية وعملائها، يمكن صياغة المتطلبات التنظيمية وهدف استرداد الاستعادة في مواجهة حالات الطوارئ، مثل نطاق إعادة الإرسال عند انتهاء الزمن (RTO) وهدف الأداء المرجعي (PRO). إضافة إلى ذلك، ينبغي أيضاً مراعاة سمات الخدمات السحابية وتصنيف الحوادث عند وضع خطة للمواجهة في حالات الطوارئ.

وتتضمن خطة المواجهة في حالات الطوارئ ما يلي:

1) التبليغ: ينبغي اتخاذ الإجراءات اللازمة للتبليغ لإخطار فريق الاستجابة وموظفي الإدارة وعملاء الخدمات السحابية المعنيين بمجرد وقوع حادث أمني.

2) تصنيف الحوادث الأمنية وتحديد درجتها: ينبغي أن ينفذ فريق المواجهة لحالات الطوارئ التقييم الأمني لحادث أمني لتحديد فئته ودرجته.

3) الاستهلال: بعد تصنيف الحوادث الأمنية وتحديد درجتها، من الملح بالنسبة إلى مقدمي الخدمات السحابية وعملائها تفعيل برنامج المواجهة المقابل المحدد مسبقاً.

4) التدابير: بعد تفعيل برنامج المواجهة، ينبغي استهلال التدابير المضادة فوراً لإزالة أثر الحوادث الأمنية. بالإضافة إلى ذلك، ينبغي بدء عمليات الاستعادة مباشرة بعد أن تتم السيطرة عملياً على الحوادث.

5) مرحلة ما بعد التخلص من الحوادث: بعد اتخاذ الإجراءات الطارئة، من المهم صياغة استنتاج بشأن أحدث المواجهات في حالات الطوارئ، بحيث تتضمن التدابير اللازمة لتحليل أسباب الحادث وتلخيصها، وإجراء تقييم للخسائر وتقييم فعالية خطة المواجهة في حالات الطوارئ وكفاءتها.

إضافةً إلى ذلك، تعتبر بعض التفاصيل أساسية بما في ذلك:

1) أعضاء فريق المواجهة في حالات الطوارئ والمسؤوليات المحددة ومعلومات الاتصال الخاصة بكل عضو من أعضاء الفريق. وبصفة عامة، يتكون فريق المواجهة في حالات الطوارئ من الموظفين الإداريين والموظفين المسؤولين عن الأعمال والموظفين التقنيين والموظفين التنظيميين.

2) نتائج تحليل التأثير التجاري (BIA) التي تنطوي على العلاقة بين الأجزاء المختلفة لنظام الحوسبة السحابية ومستوى الأولوية للمكونات الرئيسية، وما إلى ذلك.

3) الإجراءات المعيارية والقوائم المرجعية لاستعادة نظام الحوسبة السحابية.

4) جرد المعدات والبرمجيات والبرمجيات الثابتة والموارد الأخرى لدعم العمليات التشغيلية اليومية لمقدمي الخدمات السحابية، بحيث يحتوي كل بند على مواصفات من قبيل الإصدارات والكميات وما إلى ذلك.

5) معلومات الاتصال الخاصة بعملاء الخدمات السحابية وإجراءات المواجهة التي تفاوض بشأنها مقدمو الخدمات السحابية وعملائها وفقاً لبند الأمن في اتفاق مستوى الخدمة للتقليل إلى أدنى حد من خسائر عملاء الخدمات السحابية خلال حادث أمني.

6) بوجه عام، لا يمكن لمقدمي الخدمات السحابية أن يتمتعوا بامتياز النفاذ إلى البيانات الخصوصية لعملاء الخدمات السحابية إلا إذا حصلوا على إذن من هؤلاء العملاء يتيح لهم القيام بذلك. وإذا أعلن عملاء الخدمات السحابية حالة الطوارئ، فقد يحتاجون إلى مساعدة مقدمي الخدمات السحابية للاستجابة بفعالية أكثر وسيعطونهم إذناً للنفاذ إلى البيانات. وكجزء من الالتزام، ينبغي لمقدمي الخدمات ألا يسيئوا استغلال إذن النفاذ إلى بيانات عملاء الخدمات السحابية.

2.9.8 مرحلة الاختبار والتنفيذ

بغية اختبار فعالية خطة المواجهة في حالات الطوارئ، ينبغي أن يُجري مقدمو الخدمات السحابية اختبارات لخطة المواجهة في حالة الطوارئ وتدريبات بشأنها، بمساعدة الموظفين ذوي الصلة المطلعين على إجراءات المواجهة. وينبغي أن يفي الاختبار والتدريبات بالمتطلبات التالية:

1) ينبغي تحديد برامج الاختبار والتدريبات مسبقاً.

2) ينبغي تسجيل العملية المفصلة للاختبار والتدريب، وينبغي إعداد تقارير لهذا الغرض.

3) يوصى مقدمو الخدمات السحابية وعملاؤها باستكمال أي اختبار مخطط على نحو مشترك كلما طرأت تغيرات مهمة ضمن إطار وضع الحوسبة السحابية أو خارجه.

وعندما تقع حوادث أمنية أو تتعطل الأعمال، ينبغي تنفيذ خطة المواجهة في حالات الطوارئ بشكل صارم بمجرد استيفاء شروط الاستهلال، وينبغي تسجيل جميع سجلات العملية أثناء عملية المواجهة لحالات الطوارئ برمتها. وبعد ذلك، وفقاً لبند الأمن في اتفاق مستوى الخدمة، ينبغي لمقدمي الخدمات السحابية أن يقدموا تقارير المواجهة لعملاء الخدمات السحابية.

واستناداً إلى نتائج الاختبار والتدريبات والتنفيذ، ينبغي مراجعة خطة المواجهة في حالات الطوارئ لزيادة فعاليتها وجدواها.

3.9.8 مرحلة الصيانة

لكي تبقى خطة المواجهة في حالات الطوارئ فعّالة، ينبغي أن تظل جاهزة على الدوام، بحيث تعكس متطلبات أنظمة الحوسبة السحابية وتعديلات اتفاق مستوى الخدمة والتغييرات في التشكيلة وحالات تغيير الموظفين. وبوجه عام، ينبغي مراجعة الخطة سنوياً لاستيعاب التغييرات في بيئة الحوسبة السحابية الفعلية. ويستند تعديل الخطة إلى العناصر التالية:

1) التغييرات في المباني والمرافق والموارد والخدمات.

2) التغييرات في متطلبات بند الأمن في اتفاق مستوى الخدمة والتشكيلة الأمنية الحرجة وتحديث البرمجيات التصحيحية المهمة وأعضاء الفريق الأساسي.

3) تقييم فعالية الخطة حسب السجلات المفصلة للتنفيذ الفعلي للخطة أثناء الاختبار والحوادث الأمنية.

10.8 تخزين النسخ الاحتياطية

تعتبر القدرة على تخزين النسخ الاحتياطية مسألة مهمة بالنسبة إلى عملاء الخدمات السحابية ومقدميها في بيئة الحوسبة السحابية. وقبل تشغيل أنشطة تخزين النسخ الاحتياطية، يحتاج مقدمو الخدمات السحابية إلى معالجة بعض المواصفات مثل:

- استراتيجية تخزين النسخ الاحتياطية بالنسبة إلى كل عميل من عملاء الخدمات السحابية أو إلى خدمة سحابية مختارة؛
- طريقة التخزين، بما في ذلك عملية التشفير أو لا؛
- موقع التخزين، ويشمل المواقع المحلية و/أو النائية؛
- فترات استبقاء البيانات الاحتياطية؛
- الإجراءات اللازمة لاختبار البيانات الاحتياطية.

وقبل اختيار مقدم الخدمات السحابية، ينبغي لعميل الخدمات السحابية أن يؤكد ما إذا كان بمقدور مقدم الخدمات السحابية هذا أن يفي ببند الأمن في اتفاق مستوى الخدمة، بما في ذلك الكفاءة الضرورية لتخزين النسخ الاحتياطية. وإذا لم يُبدِ مقدم الخدمات السحابية الكفاءة اللازمة لتخزين النسخ الاحتياطية، ينبغي لعميل الخدمات السحابية أن ينظر بشكل كامل في وضع استراتيجية لتخزين النسخ الاحتياطية وتنفيذها. وبخلاف ذلك، إذا أبدى مقدم الخدمات السحابية الكفاءة اللازمة لتخزين النسخ الاحتياطية، ينبغي لعميل الخدمات السحابية حينذاك أن يتعاون معه للقيام بعمليات تخزين النسخ الاحتياطية.

وينبغي لمقدم الخدمات السحابية أن يُطلع عملاء الخدمات السحابية على التفاصيل الأساسية لآلية تخزين النسخ الاحتياطية. وعند التعامل مع النسخ الاحتياطية، ينبغي أن يعالج مقدمو الخدمات السحابية المواصفات للوفاء بكل مطلب من المتطلبات التالية لعملاء الخدمات السحابية:

1) استراتيجية تخزين النسخ الاحتياطية: لما كان لكل عميل من عملاء الخدمات السحابية احتياجات فردية فيما يتعلق بتخزين النسخ الاحتياطية، فمن الضروري النظر في المقام الأول في العوامل ذات الصلة، والتي تشمل ما يلي:
   - أهداف معقولة لنقطة الاستعادة (RPO) ووقت الاستعادة (RTO). ويشير هدف نقطة الاستعادة إلى المدة الزمنية التي تفصل بين نشاطين من أنشطة تخزين النسخ الاحتياطية، في حين تعكس أهداف وقت الاستعادة الوقت اللازم للعودة إلى تخزين النسخ الاحتياطية.
   - سياسة معقولة للاحتفاظ بالبيانات: ينبغي لهذه السياسة أن تحدد عدد النسخ الاحتياطية.
   - جمع معقول بين النسخ الاحتياطي على مستوى الملف والنسخ الاحتياطي على مستوى الآلة الافتراضية: وينبغي أن يحقق الجمع بينهما كلفة استثمارية مثلى، وهو أمر يستند إلى هدف نقطة الاستعادة وأهداف وقت الاستعادة.
   - جمع معقول بين تخزين النسخ الاحتياطية في الموقع وخارجه: يتم تخزين النسخ الاحتياطية في الموقع المحلي، الأمر الذي يمكن أن يلبي الحاجة إلى الاستعادة السريعة إثر وقوع الأعطال الكبرى. ويتم تخزين النسخ الاحتياطية خارج الموقع في موقع بعيد، وهو أمر ضروري لمواجهة الأعطال الكبرى. ويعتمد الجمع بينهما على متطلب بند الأمن في اتفاق مستوى الخدمة، وكلفة الاستثمار.
   - إجراءات الاختبار المنتظم للاستعادة: يعتبر اختبار الاستعادة الأسلوب المطلق للتحقق من صلاحية أي نسخة من النسخ الاحتياطية.
2) ترتيب المهام: بمجرد تحديد استراتيجية تخزين النسخ الاحتياطية، ينبغي لمقدمي الخدمات السحابية أن يضطلعوا بوضع ترتيب مناسب للمهام بشأن عمليات تخزين النسخ الاحتياطية. وبغية خفض تأثر أداء البنية التحتية للحوسبة السحابية، ينبغي أن يعتمد ترتيب مهام تخزين النسخ الاحتياطية على متطلبات عملاء الخدمات السحابية بشأن تخزين النسخ الاحتياطية وأنماط الحركة في الشبكة وكفاءة مقدمي الخدمات السحابية فيما يتعلق بتخزين النسخ الاحتياطية.

3) إجراءات التحقق من صلاحية النسخ الاحتياطية: إن إنجاز نسخة بيانات كاملة وصحيحة يعني تحقيق عملية نسخ احتياطي. وبوجه عام، ينبغي أن تتضمن الإجراءات الخطوتين الأساسيتين التاليتين:

- استخدام دالة الفرم وحيدة الاتجاه للتحقق من أن النسخ الاحتياطية توافق البيانات الأصلية. وإذا كانت النسخ الاحتياطية مماثلة للبيانات الأصلية، يمكن إذ ذاك الانتقال إلى الخطوة التالية. بالإضافة إلى ذلك، يمكن استخدام طريقة التوقيع الرقمي للتحقق من مشغّل النسخ الاحتياطي، الأمر الذي يمكن أن يعود ببعض الفائدة على إدارة عملية النسخ الاحتياطي.
- إجراء اختبار استعادة للنسخ الاحتياطي. نظراً إلى التغير المستمر في بيئة الحوسبة السحابية، يعتبر الاختبار المنتظم للاستعادة أمراً بالغ الأهمية.

4) الاحتراز من لقطات الآلة الافتراضية: في سيناريو الحوسبة السحابية، يقدم أسلوب أخذ اللقطات وسيلة سريعة وسهلة للعودة إلى المستوى السابق، إذ يمكنه أن يقوم بدور أسلوب تخزين النسخ الاحتياطية إلى حد ما. ومع ذلك، ينبغي عدم استخدام أسلوب أخذ اللقطات بصورة متكررة، وذلك للأسباب التالية:

- تسمح اللقطات للبيانات ذاتها بالازدياد وبأن تُكتب في ملفات اللقطات المختلفة، ما يمكن أن يؤدي بسهولة إلى ترد خطير في الأداء وإشغال سريع للحيز المخصّص للتخزين في أنظمة الحوسبة السحابية.
- وبغية الحد من إشغال الحيز المخصص للتخزين، غالباً ما تُشكل سلسلة من اللقطات الأصلية للآلة الافتراضية لكي تحوي ما يختلف عن اللقطة الأولى فحسب. وبمجرد إزالة اللقطة الأولى، فإن اللقطات المتتالية ستكون غير صالحة في نهاية المطاف. وتزداد المخاطر الأمنية مع تزايد معدل اللقطات المتتالية.

11.8 التدقيق الأمني الداخلي

نظراً إلى الطائفة الواسعة من عمليات التدقيق الأمنية، لا تركز هذه التوصية إلا على التدقيق الأمني الداخلي من منظور أمن التشغيل. ويمكن لتدقيق أمني موثوق وموضوعي أن يساعد على ضمان إجراء اختبارات ومراجعات دقيقة لأنشطة إدارة المخاطر التشغيلية، لتعزيز شفافية خدمات الحوسبة السحابية، بل وحتى تلبية المتطلبات التنظيمية.

1.11.8 متطلبات التدقيق الأمني

لضمان موضوعية التدقيق الأمني وموثوقيته، ينبغي لمقدمي الخدمات السحابية وعملاء الخدمات السحابية أن يتفاوضوا للتوصل إلى اتفاق بشأن استخدام إطار مشترك لمراقبة تكنولوجيا المعلومات وضمان شهاداتها، ووسائل جمع وتخزين وتقاسم سجل التدقيق (من قبيل سجلات النظام وتقارير الأنشطة وتشكيلات النظام). ووفقاً لبند الأمن في اتفاق مستوى الخدمة المبرم بين مقدمي الخدمات السحابية وعملاء الخدمات السحابية، ينبغي التخطيط للتدقيق الأمني واستهدافه لتلبية بعض المتطلبات:

1) الفريق والوظائف: أولاً، ينبغي أن يضم أعضاء فريق التدقيق الإدارة العليا وموظفين من مختلف إدارات الأعمال (الإدارية والتقنية) لضمان نزاهة الموارد وجدولتها أثناء عملية التدقيق. ثانياً، ينبغي أن يشمل هدف التدقيق التحقق من معمارية إدارة أمن مقدمي الخدمات السحابية و/أو عملاء الخدمات السحابية، والتحقق من فعالية وصحة التدابير المتخذة للسيطرة على المخاطر. ثالثاً، ينبغي لفريق التدقيق أن يراقب عملية التدقيق التي ينبغي أن تمتثل لمسار الأعمال المقيّس. وأخيراً، ينبغي إجراء التدقيق الأمني عدة مرات في فترة ملائمة.

2) متطلبات عملية التدقيق: أولاً، واستناداً إلى ما سلف، ينبغي تسجيل أنشطة التدقيق بالكامل والتخطيط لها بشكل جيد لتجنب تعطل سير أعمال مقدمي الخدمات السحابية وعملاء الخدمات السحابية. ثانياً، ينبغي تحديد نطاق أهداف التدقيق والموارد المطلوبة بوضوح وضمان تيسرها. وأخيراً، ينبغي توثيق جميع إجراءات ومتطلبات التدقيق، فضلاً عن مسؤوليات أعضاء فريق التدقيق.

3) حماية أدوات التدقيق: ينبغي تقييد استخدام أدوات التدقيق وتقييسها لتجنب سوء استخدام موارد الحوسبة السحابية.

2.11.8 المتطلبات الخاصة للتدقيق

بالمقارنة مع إجراءات التدقيق الأمني في أنظمة المعلومات التقليدية، يُطلب من أعضاء فريق التدقيق بوجه خاص أن يكونوا على دراية بالتحديات التي يطرحها التمثيل الافتراضي وتكنولوجيات الحوسبة السحابية. وفي الوقت نفسه، تحتاج فئة التدقيق إلى توسيع نطاقها من سجلات الأمن التقليدي إلى تشغيل وصيانة البيانات وبيانات الأعمال، بل وحتى موقع تخزين بيانات المستخدم. وتتضمن بنود التدقيق، دون أن تقتصر على ذلك، ما يلي:

1) تدقيق أمن التمثيل الافتراضي: تشمل متطلبات التدقيق الرئيسية وسائل التشفير والتحقق من سلامة ملفات الصور الافتراضية وعزل مختلف الآلات الافتراضية وتعزيزها ومراقبة النفاذ إلى الآلات الافتراضية وانتقالها ورصد عمليات الآلات الافتراضية ومعاينة مواطن الضعف الكامنة فيها ورصد الحركة الداخلية والتدابير المتخذة بشأن الشبكات الافتراضية.

2) تدقيق أمن معمارية المنصة السحابية ومكوناتها: من الأهمية بمكان تدقيق الأساس المنطقي للتدابير المضادة وفعاليتها، بما في ذلك سياسة تقسيم الميدان الأمني ومضاعفة أمن معمارية الشبكة والمكونات الرئيسية ومسح مواطن الضعف وتعزيز الأمن وتجميع البرمجيات التصحيحية وتوزيعها وتشكيلات نظام منع التسلل (IPS)/نظام كشف التسلل (IDS) وجدران الحماية وأجهزة أمن التمثيل الافتراضي.

3) تدقيق عمليات التشغيل والصيانة والسلوك التجاري: تركز متطلبات التدقيق أساساً على سجلات التشغيل والصيانة وسجلات النفاذ التجاري والنفاذ إلى البيانات وفحص السلوك التجاري.

4) تدقيق إدارة خدمات الهوية (IAM) والنفاذ ومراقبة النفاذ: تعتبر متطلبات التدقيق حيوية لضمان التشغيل السليم في بيئة الحوسبة السحابية، التي تشمل تصميم ونشر الاستيقان متعدد العوامل ومراقبة النفاذ والتسجيل الوحيد للدخول (SSO) والفصل بين الواجبات وإدارة المستخدمين المميزين.

5) تدقيق إدارة المفاتيح وتشفير البيانات: نظراً إلى أن التشفير يعتبر آلية أساسية لحماية البيانات في بيئة الحوسبة السحابية بغض النظر عما إذا كان أسلوب الخدمة من نوع البنية التحتية كخدمة (IaaS) أو المنصات كخدمة (PaaS) أو حتى البرمجيات كخدمة (SaaS)، ينبغي أن تشمل متطلبات التدقيق تنفيذ ومعالجة إدارة المفاتيح وتشفير البيانات.

6) تدقيق مواجهة حالات الطوارئ وإدارتها: تركز متطلبات التدقيق أساساً على وضع خطة للطوارئ وإنشاء إدارة مركزية للحوادث الأمنية وإجراء تحليل للترابط بين الحوادث الأمنية المختلفة.

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.810]	Recommendation ITU-T X.810 (1995) | ISO/IEC 10181-1:1996, *Information technology – Open Systems Interconnection – Security frameworks for open systems: Overview*.
[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-ITU-T Y.3510]	Recommendation ITU-T Y.3510 (2016), *Cloud computing infrastructure requirements*.
[b-ISO/IEC DIS 19086-1]	ISO/IEC DIS 19086-1: 2016, *Information technology – Cloud computing – Service level agreement (SLA) framework and technology – Part 1: Overview and concepts*.
[b-ISO/IEC 20000-1]	ISO/IEC 20000-1:2011, *Information technology – Service management – Part 1: Service management system requirements*.
[b-ISO/IEC 27000]	ISO/IEC 27000:2012, *Information technology – Security techniques – Information security management systems – Overview and vocabulary*.
[b-ISO/IEC DIS 27017]	ISO/IEC DIS 27017:2015 , *Information technology – Security techniques – Code of practice for information security controls based on ISO/IEC 27002 for cloud services*.
[b-ISO 27729]	ISO 27729:2012, *Information and documentation – International standard name identifier (ISNI)*
[b-NIST-SP-800-30]	NIST Special Publication 800-30 Rev. 1 (2012), *Guide for Conducting Risk Assessments*.

سلاسل التوصيات الصادرة عن قطاع تقييس الاتصالات

السلسلة A	تنظيم العمل في قطاع تقييس الاتصالات
السلسلة D	المبادئ العامة للتعريفة
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	المطاريف وطرائق التقييم الذاتية والموضوعية
السلسلة Q	التبديل والتشوير
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، 2017