الاتحاد الدولي للاتصالات

ITU-T X.1601

(2014/01)

قطاع تقييس الاتصالات
في الاتحاد الدولي للاتصالات

السلسلة X: شبكات البيانات والاتصالات بين الأنظمة المفتوحة ومسائل الأمن

أمن الحوسبة السحابية – نظرة عامة على أمن الحوسبة السحابية

إطار أمني للحوسبة السحابية

التوصية ITU-T X.1601

توصيات السلسلة X الصادرة عن قطاع تقييس الاتصالات

شبكات البيانات والاتصالات بين الأنظمة المفتوحة ومسائل الأمن

الشبكات العمومية للبيانات	X.199–X.1
التوصيل البيني للأنظمة المفتوحة	X.299–X.200
التشغيل البيني للشبكات	X.399–X.300
أنظمة معالجة الرسائل	X.499–X.400
الدليل	X.599–X.500
التشغيل البيني لأنظمة التوصيل OSI ومظاهر النظام	X.699–X.600
إدارة التوصيل البيني للأنظمة المفتوحة (OSI)	X.799–X.700
الأمن	X.849–X.800
تطبيقات التوصيل البيني للأنظمة المفتوحة (OSI)	X.899–X.850
المعالجة الموزعة المفتوحة	X.999–X.900
أمن المعلومات والشبكات	
الجوانب العامة للأمن	X.1029–X.1000
أمن الشبكة	X.1049–X.1030
إدارة الأمن	X.1069–X.1050
الخصائص البيومترية	X.1099–X.1080
تطبيقات وخدمات آمنة	
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
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.

إطار أمني للحوسبة السحابية

ملخص

تقدم التوصية ITU-T X.1601 وصفاً للإطار الأمني للحوسبة السحابية. وتجري التوصية تحليلاً للتهديدات والتحديات الأمنية في بيئة الحوسبة السحابية، وتصف القدرات الأمنية التي يمكنها التخفيف من حدة هذه التهديدات والتصدي للتحديات الأمنية. وتُعرض منهجية إطارية لتحديد القدرات الأمنية التي تتطلب وضع مواصفات من أجل التخفيف من حدة التهديدات الأمنية والتصدي للتحديات الأمنية للحوسبة السحابية. ويوفر التذييل I جدول تقابل بشأن كيفية التصدي لتهديد أو تحدٍّ أمني معين باستخدام واحدة أو أكثر من القدرات الأمنية المقابلة.

التسلسل التاريخي

الصيغة	التوصية	تاريخ الموافقة	لجنة الدراسات	معرف الهوية الفريد*
1.0	ITU-T X.1601	2014-01-24	17	11.1002/1000/12036-en

الكلمات الأساسية

حوسبة سحابية، حماية الخصوصية، قدرات أمنية، تحديات أمنية، إطار أمني، تهديدات أمنية.

* للنفاذ إلى التوصية، اطبع العنوان الإلكتروني: http://handle.itu.int/ في حقل العنوان من متصفح الويب الذي تستعمله، متبوعاً بحرف الهوية الفريد للتوصية. ومثال على 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 رقم 1 الصادر عن الجمعية العالمية لتقييس الاتصالات.

وفي بعض مجالات تكنولوجيا المعلومات التي تقع ضمن اختصاص قطاع تقييس الاتصالات، تعد 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 المعطيات الخاصة ببراءات الاختراع في مكتب تقييس الاتصالات (TSB) في الموقع http://www.itu.int/ITU-T/ipr/.

جدول المحتويات

الصفحة

1 مجال التطبيق 1
2 المراجع 1
3 المصطلحات والتعاريف 1
1.3 مصطلحات معرّفة في وثائق أخرى 1
2.3 المصطلحات المعرفة في هذه التوصية 2
4 المختصرات 3
5 اصطلاحات 4
6 لمحة عامة 4
7 التهديدات الأمنية للحوسبة السحابية 5
1.7 التهديدات الأمنية لعملاء الخدمة السحابية (CSC) 5
2.7 التهديدات الأمنية لمقدمي الخدمات السحابية (CSP) 6
8 التحديات الأمنية للحوسبة السحابية 7
1.8 التحديات الأمنية لعملاء الخدمة السحابية (CSC) 7
2.8 التحديات الأمنية لمقدمي الخدمات السحابية (CSP) 9
3.8 التحديات الأمنية للشريك في الخدمة السحابية (CSN) 11
9 قدرات الأمن في الحوسبة السحابية 11
1.9 نموذج الثقة 11
2.9 إدارة خدمات الهوية والنفاذ (IAM)، والاستيقان والترخيص ومراجعة العمليات 12
3.9 الأمن المادي 12
4.9 أمن السطوح البينية 12
5.9 أمن التمثيل الافتراضي للحوسبة 12
6.9 أمن الشبكات 13
7.9 عزل البيانات وحمايتها وحماية الخصوصية 13
8.9 التنسيق الأمني 14
9.9 الأمن التشغيلي 14
10.9 إدارة الحوادث 14
11.9 التعافي من الأعطال الكبرى 14
12.9 تقييم أمن الخدمات ومراجعته 15
13.9 قابلية التشغيل البيني وقابلية النقل وقابلية الرجوع 15
14.9 أمن سلسلة التوريد 15
10 منهجية إطارية 16
التذييل I – جدول التقابل بين التهديدات والتحديات الأمنية للحوسبة السحابية والقدرات الأمنية 19
بيبليوغرافيا 23

التوصية ITU-T X.1601

إطار أمني للحوسبة السحابية

1 مجال التطبيق

تقدم هذه التوصية تحليلاً للتهديدات والتحديات الأمنية في بيئة الحوسبة السحابية وتعطي وصفاً للقدرات الأمنية التي يمكن أن تخفف من حدة هذه التهديدات وتتصدى للتحديات الأمنية. كما تقدم منهجية إطارية لتحديد القدرات الأمنية التي تتطلب وضع مواصفات من أجل التخفيف من حدة التهديدات الأمنية والتصدي للتحديات الأمنية للحوسبة السحابية.

2 المراجع

لا توجد.

3 المصطلحات والتعاريف

1.3 مصطلحات معرّفة في وثائق أخرى

تعرِّف هذه التوصية المصطلحات التالية المعرَّفة في وثائق أخرى:

1.1.3 استيقان [b-NIST-SP-800-53]: التحقّق من هوية المستعمل أو العملية أو الجهاز، غالباً كشرط أساسي للسماح بالنفاذ إلى الموارد في نظام المعلومات.

2.1.3 قدرة [b-ISO/IEC 19440]: القدرة على أداء نشاط معين.

3.1.3 مراقب البيانات [b-key definition]: شخص يحدد (بمفرده أو بالاشتراك مع أشخاص آخرين) الغرض الذي من أجله تمت معالجة أي معلومات شخصية، أو تقرر معالجتها، وكيفية القيام بذلك.

4.1.3 معالج البيانات [b-key definition]: فيما يتعلق بالبيانات الشخصية، يقصد به أي شخص (غير الموظف أو مراقب البيانات) يعالج البيانات بالنيابة عن مراقب البيانات.

5.1.3 مشرف أعلى [b-NIST-SP-800-125]: مكوّنة التمثيل الافتراضي التي تدير أنظمة التشغيل الخاصة بالضيوف على حاسوب مضيف وتتحكم بتدفق التعليمات بين أنظمة التشغيل الخاصة بالضيوف والتجهيزات المادية.

6.1.3 المعلومات المحدِّدة لهوية شخص [b-ISO/IEC 29100]: معلومات أ) يمكن أن تستخدم للتعرّف إلى هوية الشخص الذي تتعلق به هذه المعلومات، أو ب) قد تكون مرتبطة بشكل مباشر أو غير مباشر بهوية الشخص المراد التعرف عليه من خلالها.

7.1.3 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.

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

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

الملاحظة 1 – يمكن أيضاً أن يُبرم الاتفاق على مستوى الخدمة بين مقدم الخدمة ومورّد أو مجموعة داخلية أو عميل يقوم بدور المورّد.

الملاحظة 2 – يمكن أن يكون الاتفاق على مستوى الخدمة مدرجاً في عقد أو أي نوع آخر من الاتفاقات الموثّقة.

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

11.1.3 آلة افتراضية (VM) [b-NIST-SP-800-145]: نسخة منطقية ومستقلة وفعالة تكون مطابقة لآلة حقيقية.

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

2.3 المصطلحات المعرفة في هذه التوصية

تعرف هذه التوصية المصطلحات التالية:

1.2.3 الحوسبة السحابية: 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.

2.2.3 خدمة سحابية: قدرة أو عدد أكبر من القدرات تُقدم عن طريق الحوسبة السحابية (الفقرة 1.2.3) وتُلبى باستخدام سطح بيني معلن.

3.2.3 عميل الخدمة السحابية: طرف (الفقرة 12.2.3) يكون مرتبطاً بعلاقة تجارية لأغراض استخدام الخدمات السحابية (الفقرة 2.2.3).

4.2.3 شريك في الخدمة السحابية: طرف يشارك في دعم أنشطة إما مقدم خدمة سحابية (الفقرة 5.2.3) أو عميل خدمة سحابية (الفقرة 3.2.3)، أو يساعد في القيام بها.

5.2.3 مقدم الخدمة السحابية: طرف (الفقرة 12.2.3) يتيح توافر الخدمات السحابية (الفقرة 2.2.3).

6.2.3 مستعمل الخدمة السحابية: شخص يرتبط بأحد عملاء الخدمة السحابية (الفقرة 3.2.3) ويستعمل الخدمات السحابية (الفقرة 2.2.3).

7.2.3 الاتصالات كخدمة (CaaS): فئة من الخدمات السحابية تكون فيها القدرة المقدّمة لعميل الخدمة السحابية (الفقرة 3.2.3) متمثلة بالاتصالات والتعاون في الوقت الفعلي.

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

8.2.3 الحوسبة السحابية المشتركة: نموذج لنشر الحوسبة السحابية يدعم حصراً مجموعة محددة من عملاء الخدمة السحابية (الفقرة 3.2.3) التي تتشارك فيه، ويتحكم في الموارد المعتمدة عضو واحد من أعضاء المجموعة على الأقل.

ملاحظة – المتطلبات المشتركة تشمل على سبيل المثال لا الحصر المهمة ومتطلبات أمن المعلومات والسياسات والاعتبارات المتعلقة بالامتثال.

9.2.3 البنية التحتية كخدمة (IaaS): فئة من الخدمات السحابية تكون فيها القدرات السحابية المقدمة لعميل الخدمة السحابية (الفقرة 3.2.3) من نوع قدرات البنية التحتية.

ملاحظة – لا يقوم عميل الخدمة السحابية (الفقرة 3.2.3) بإدارة الموارد المادية أو الافتراضية الأساسية أو بالتحكم بها بل تكون لديه سيطرة على أنظمة التشغيل والخزن والتطبيقات المنتشرة التي تستخدم الموارد المادية والافتراضية. وقد تتوفر لدى عميل الخدمة السحابية (الفقرة 3.2.3) أيضاً قدرة محدودة على التحكم ببعض مكونات الربط الشبكي (مثل جدران الحماية لدى المضيف).

10.2.3 تعدد الشاغلين: توزيع الموارد المادية والافتراضية بحيث يتم عزل الشاغلين المتعددين (الفقرة 18.2.3) وحساباتهم وبياناتهم عن بعضهم البعض، ويكون النفاذ غير ممكن فيما بين بعضهم البعض.

11.2.3 الشبكة كخدمة (NaaS): فئة من الخدمات السحابية تكون فيها القدرة المقدمة لعميل الخدمة السحابية (الفقرة 3.2.3) متمثلة في قدرة توصيلية النقل والقدرات المتصلة بالشبكات.

ملاحظة – يمكن أن توفر الشبكة كخدمة أياً من أنواع القدرات السحابية الثلاثة.

12.2.3 طرف: شخص طبيعي أو منظمة.

13.2.3 المنصات كخدمة (PaaS): فئة من الخدمات السحابية تكون فيها القدرات السحابية المقدمة لعميل الخدمة السحابية (الفقرة 3.2.3) من نوع قدرات المنصة.

14.2.3 الخدمة السحابية الخاصة: نموذج لنشر الحوسبة السحابية يشارك فيه حصراً عميل واحد للخدمة السحابية (الفقرة 3.2.3) ويتم في إطاره التحكم بالموارد من قبل عميل الخدمة السحابية (الفقرة 3.2.3).

15.2.3 الخدمة السحابية العامة: نموذج لنشر الحوسبة السحابية يُحتمل أن يتوفر لأي عميل من عملاء الخدمة السحابية (الفقرة 3.2.3) ويتم في إطاره التحكم بالموارد من قبل مقدم الخدمة السحابية (الفقرة 5.2.3).

16.2.3 تحدٍّ أمني: "عقبة" أمنية مختلفة عن التهديدات الأمنية المباشرة، تنجم عن طبيعة الخدمات السحابية وبيئتها التشغيلية، بما في ذلك التهديدات "غير المباشرة". انظر الفقرتين 7 و8.

17.2.3 البرمجيات كخدمة (SaaS): فئة من الخدمات السحابية تكون فيها القدرات السحابية المقدمة لعميل الخدمة السحابية (الفقرة 3.2.3) من نوع قدرات التطبيقات.

18.2.3 شاغل: مجموعة من مستعملي الخدمات السحابية (الفقرة 6.2.3) الذين يتقاسمون مجموعة من الموارد المادية والافتراضية.

ملاحظة – في إطار تعدد الشاغلين (الفقرة 10.2.3)، عادة ما تنتمي مجموعة مستعملي الخدمة السحابية (الفقرة 6.2.3) التي تشكل شاغلاً إلى منظمة عملاء الخدمة السحابية نفسها (الفقرة 3.2.3). وقد توجد حالات تشتمل فيها مجموعة مستعملي الخدمة السحابية (الفقرة 6.2.3) على مستعملين ينتمون إلى عدة عملاء مختلفين، ولا سيما في حالة نشر الخدمة السحابية المشتركة (الفقرة 8.2.3)، لكن هذه تمثل استثناءات محددة. ومع ذلك فقد يكون لإحدى منظمات عملاء الخدمة السحابية (الفقرة 3.2.3) عدد كبير من الشاغلين المختلفين الذين لديهم مقدم واحد للخدمة السحابية (الفقرة 5.2.3)، ويمثلون ربما مجموعات تجارية مختلفة داخل المنظمة (مثلاً المبيعات مقابل المحاسبة)، وذلك نتيجة احتمال وجود سبب وجيه لإبقاء البيانات والأنشطة الخاصة بتلك المجموعات المختلفة منفصلة بصورة تامة لأسباب تتعلق بالأعمال التجارية والتجارة.

4 المختصرات

تستخدم هذه التوصية المختصرات التالية:

API سطح بيني لبرمجة التطبيقات *(Application Programming Interface)*

BCP خطة الاستمرارية التجارية *(Business Continuity Plan)*

CaaS الاتصالات كخدمة *(Communications as a Service)*

CPU وحدة المعالجة المركزية *(Central Processing Unit)*

CSC عميل الخدمة السحابية *(Cloud Service Customer)*

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

CSP مقدم الخدمة السحابية *(Cloud Service Provider)*

CSU مستعمل الخدمة السحابية *(Cloud Service User)*

DNS نظام أسماء الميادين *(Domain Name System)*

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

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

ICT تكنولوجيا المعلومات والاتصالات *(Information and Communication Technology)*

IP بروتوكول الإنترنت *(Internet Protocol)*

IT تكنولوجيا المعلومات *(Information Technology)*

NaaS الشبكات كخدمة *(Network as a Service)*

OS نظام التشغيل *(Operating System)*

PaaS المنصات كخدمة *(Platform as a Service)*

PII المعلومات المحددة لهوية شخص *(Personally Identifiable Information)*

PKI البنية التحتية للمفاتيح العمومية *(Public Key Infrastructure)*

SaaS البرمجيات كخدمة *(Software as a Service)*

SIM وحدة هوية المشترك *(Subscriber Identity Module)*

SLA اتفاق على مستوى الخدمة *(Service Level Agreement)*

VM آلة افتراضية *(Virtual Machine)*

5 اصطلاحات

لا توجد.

6 لمحة عامة

الحوسبة السحابية هي نموذج لتمكين مستعمل الشبكة من النفاذ الشبكي بسهولة وعند الحاجة إلى مجموعة مشتركة من الموارد القابلة للتشكيل (مثل الشبكات والمخدّمات والتخزين والتطبيقات والخدمات)، التي يمكن توفيرها وإطلاقها بسرعة وبأدنى حد من الجهد الإداري أو التفاعل من جانب مقدم الخدمة. ويستطيع مستعملو الحوسبة السحابية استخدام هذه الموارد لتطوير واستضافة وتنفيذ الخدمات والتطبيقات عند الحاجة وبطريقة مرنة في أي نوع من الأجهزة، وفي أي وقت ومن كل مكان داخل بيئة الحوسبة السحابية. وتُقدَّم خدمات الحوسبة السحابية عادة ضمن فئات معينة من الخدمات، مثل البنية التحتية كخدمة (IaaS) والمنصات كخدمة (PaaS) والبرمجيات كخدمة (SaaS) والشبكات كخدمة (NaaS) وما إلى ذلك. وهذه الفئات من الخدمات تمكّن عملاء الخدمة السحابية من إطلاق أعمالهم التجارية أو تغييرها بسرعة وسهولة من دون إنشاء بنية تحتية وأنظمة جديدة لتكنولوجيا المعلومات والاتصالات (ICT)، ومن تأمين الفرص لتوفير الموارد بطريقة مرنة حسب الحاجة. فعلى سبيل المثال، قد يوفر بعض مقدمي الخدمات السحابية (CSP) موارد مستخلصة من التجهيزات والبرمجيات يمكن عرضها كخدمة (مثلاً البنية التحتية كخدمة (IaaS) أو الشبكات كخدمة (NaaS)). وقد يوفر غيرهم من مقدمي الخدمات السحابية منصات (PaaS) أو تطبيقات (SaaS) محددة للخدمة السحابية لتمكين العملاء والشركاء من القيام بسرعة بوضع ونشر تطبيقات جديدة يمكن تشكيلها واستعمالها عن بُعد.

وينطوي اعتماد الحوسبة السحابية على وجود تهديدات ومخاطر أمنية، علماً بأن متطلبات الأمن تتغير إلى حد بعيد تبعاً للنماذج المختلفة لنشر الخدمات السحابية وفئات هذه الخدمات. فالطبيعة الموزعة والمتعددة الشاغلين للحوسبة السحابية، وغلبة النفاذ عن بُعد إلى خدمات الحوسبة السحابية، وعدد الكيانات التي تشترك في كل عملية، تشكل كلها عوامل تجعل الحوسبة السحابية بطبيعتها أكثر عرضة من غيرها من النماذج للتهديدات الأمنية الداخلية والخارجية. ويمكن التخفيف من حدة الكثير من التهديدات الأمنية بتطبيق العمليات والآليات الأمنية التقليدية. والأمن يطال أجزاء كثيرة من خدمات الحوسبة السحابية ويؤثر فيها. ولذلك تعتبر إدارة خدمات الحوسبة السحابية، بالإضافة إلى الموارد المرتبطة بها، أحد الجوانب الأساسية للحوسبة السحابية.

وقبل الانتقال من نظام تكنولوجيا المعلومات والاتصالات إلى الحوسبة السحابية، يتعين على عميل الحوسبة السحابية (CSC) المحتمل أن يتعرف إلى التهديدات الأمنية (انظر الفقرة 7 أدناه) والتحديات الأمنية (انظر الفقرة 8) التي يتعرض إليها.

وبالاستناد إلى هذه التهديدات والتحديات، يتم تحديد مجموعة من القدرات الأمنية الرفيعة المستوى (انظر الفقرة 9). ومع أن المتطلبات المحددة لهذه القدرات تقع خارج نطاق هذه التوصية، إلا أن ثمة حاجة إلى تحديدها بالنسبة لحالات محددة من تنفيذ خدمات الحوسبة السحابية، وبالاستناد إلى تقييم المخاطر الناجمة عن التهديدات والتحديات التي حُدّدت.

واعتماداً على تقييم المخاطر، يستطيع عميل الخدمة السحابية أن يحدد ما إذا كان سيعتمد الحوسبة السحابية وأن يتخذ قرارات مستنيرة بشأن مقدمي الخدمات والمعمارية. وينبغي إجراء تقييم المخاطر المذكور أعلاه باستعمال إطار لإدارة مخاطر أمن المعلومات (مثل إطار إدارة المخاطر المحدد في [b-ISO/IEC 27005]. انظر أيضاً الفقرة 10 أدناه بشأن المنهجية الإطارية المقترحة.

وتميز هذه التوصية بين التهديدات الأمنية والتحديات الأمنية. فالتهديدات الأمنية هي التي تكون مرتبطة بالهجمات (الفاعلة منها والمنفعلة)، وكذلك بالإخفاقات البيئية والكوارث. أما التحديات الأمنية فتشمل المصاعب الناجمة عن طبيعة الخدمات السحابية وبيئتها التشغيلية. وإذا لم يتم التصدي للتحديات الأمنية على نحو سليم، فإنها قد تترك الأبواب مشرعة أمام التهديدات.

وبناءً على هذه التهديدات والتحديات الأمنية المحددة، يجري وصف القدرات الأمنية الرامية إلى التخفيف من حدة التهديدات الأمنية للحوسبة السحابية والتصدي للتحديات الأمنية المتعلقة بها.

7 التهديدات الأمنية للحوسبة السحابية

للتهديدات القدرة على إلحاق الضرر بالأصول كالمعلومات والعمليات والأنظمة وبالتالي بالمنظمات. وقد تنشأ التهديدات من مصدر طبيعي أو بشري، وقد تكون عرضية أو متعمدة. وقد يصدر التهديد من داخل المنظمة أو من خارجها. ويمكن تصنيف التهديدات تبعاً لما إذا كانت عرضية أو متعمدة، وقد تكون فاعلة أو منفعلة.

وتعتمد التهديدات المحددة التي نواجهها اعتماداً كبيراً على الخدمة السحابية المحددة المختارة. فبالنسبة للخدمة السحابية العامة مثلاً، يمكن أن تنشأ التهديدات من تقسيم المسؤوليات بين عميل الخدمة السحابية ومقدم الخدمة السحابية: التعقيدات التي تتخلل تحديد الولاية القضائية على البيانات والعمليات، واتساق حماية البيانات وكفايتها، والحفاظ على الخصوصية، وما إلى ذلك. بيد أن التصدي للتهديدات التي تواجه الخدمة السحابية الخاصة أكثر بساطة لأن عميل الخدمة السحابية هو الذي يتحكم في جميع الشاغلين المستضافين من قبل مقدم الخدمة السحابية. وعلى الرغم من أن الوثائق القائمة الصادرة عن الدوائر الصناعية تشمل أيضاً بعض التهديدات المحددة في هذه التوصية (مثل التوصية ITU-T X.800)، فلجميع التهديدات أهمية بالنسبة للحوسبة السحابية. وتتوقف إمكانية تطبيق كل تهديد من التهديدات على الخدمة السحابية المختارة.

وتقدم هذه الفقرة وصفاً للتهديدات الأمنية المختلفة التي يمكن أن تنشأ في بيئة الحوسبة السحابية.

1.7 التهديدات الأمنية لعملاء الخدمة السحابية (CSC)

تمثل التهديدات التالية تلك التي تؤثر في عملاء الخدمة السحابية تأثيراً مباشراً. وقد تؤثر في المصالح التجارية لعملاء الخدمة السحابية أو في خصوصيتهم أو مشروعيتهم أو سلامتهم. وليس جميع عملاء الخدمة السحابية معرضين للأخطار كافة. فالتفاوت في الخطر يعتمد على طبيعة عميل الخدمة السحابية والخدمة السحابية المستعملة. وعلى سبيل المثال فإن الخدمة السحابية المخصصة لتحويل شفرة الملفات الفيديوية التجارية لا تفرض أي متطلبات لحماية المعلومات المحددة لهوية الشخص (PII)، ولكنها تفرض متطلبات شديدة بشأن حماية الأصول الرقمية.

1.1.7 فقدان البيانات وتسربها

بما أن الخدمة السحابية هي عادةً خدمة متعددة الشاغلين، فإن فقدان البيانات أو تسربها يشكل تهديداً خطيراً لعميل الخدمة السحابية. فقد يسبب غياب الإدارة المناسبة لمعلومات التجفير، مثل مفاتيح التجفير وشفرات الاستيقان وامتيازات النفاذ، أضراراً بالغة مثل فقدان البيانات وتسربها غير المتوقع إلى الخارج. وعلى سبيل المثال فإن النقص في الاستيقان والترخيص وضوابط المراجعة، والاستعمال غير المتوافق لمفاتيح التجفير و/أو الاستيقان، والإخفاقات التشغيلية، ومشاكل التخلص من المخلّفات، والمسائل القضائية والسياسية، ومصداقية مركز البيانات، والتعافي من الأعطال، هي كلها عوامل يمكن اعتبارها مصادر كبيرة لهذا التهديد ويمكن ربطها بالتحديات الواردة في الفقرات 2.1.8 "فقدان الثقة"، و3.1.8 "غياب الإدارة"، و4.1.8 "فقدان الخصوصية".

2.1.7 النفاذ غير الآمن للخدمات

تكون أوراق اعتماد الهوية، بما فيها تلك المتعلقة بمسؤولي عملاء الخدمة السحابية، عرضة بوجه خاص للمستعملين غير المرخص لهم في البيئة عالية التوزيع للحوسبة السحابية، وذلك لأنه على خلاف الاتصالات التقليدية، يكون من الصعب في الغالب الاعتماد على الموقع (مثل الخط الأرضي الثابت) أو على وجود عنصر محدد من عناصر التجهيزات (مثل وحدة هوية المشترك المتنقل (SIM)) لتعزيز الاستيقان بشأن الهوية. ولأن معظم العروض المتعلقة بالخدمة تتم عن بُعد، فإن التوصيلات غير المحمية تكشف عن احتمال وجود موطن ضعف. وحتى عندما تكون التوصيلات محمية أو محلية، فقد تنجح أيضاً أساليب الهجمات الأخرى (من قبيل التصيّد الاحتيالي والاحتيال والتحايل الاجتماعي واستغلال مواطن ضعف البرمجيات). فلو استطاع أحد المهاجمين النفاذ إلى بيانات اعتماد هوية المستعملين أو المسؤولين، فسيكون في وسعه التنصت على الأنشطة والعمليات، والتلاعب بالبيانات، وإعادة معلومات زائفة، وإعادة توجيه زبائن عميل الخدمة السحابية إلى مواقع غير شرعية. وغالباً ما يعاد استعمال كلمات السر في مواقع إلكترونية وخدمات متعددة، ما يفاقم أثر هذه الهجمات لأن اقتحاماً واحداً من شأنه تعريض عدة خدمات للاقتحام. كما أن الحلول التي تطرحها الحوسبة السحابية تضيف تهديداً جديداً إلى المشهد. فقد يصبح حساب عميل الخدمة السحابية وحالات تقديم الخدمة قاعدة جديدة لأحد المهاجمين. وانطلاقاً من هذه النقطة، قد يستفيد المهاجم من السمعة الجيدة لعميل الخدمة السحابية وموارده لإطلاق هجمات لاحقة.

3.1.7 التهديدات داخلية المصدر

عندما يتعلق الأمر ببني البشر، يبرز على الدوام خطر قيام الأفراد بالتصرف بطريقة لا تتوافق مع ضمان أمن الخدمة. فمشاركة موظفي عميل الخدمة السحابية في كلمات السر الخاصة "بمسؤول" الخدمة أو ترك أوراق الاعتماد غير آمنة (مدونة مثلاً على قصاصات ملصقة على الشاشة)، أو وجود مستعملين لا مبالين أو غير مدربين بالقدر الكافي (أو أفراد العائلة في حالة العميل)، أو الأفعال الخبيثة التي يقوم بها بعض الموظفين الناقمين، هي أمور تشكل دائماً تهديداً كبيراً.

2.7 التهديدات الأمنية لمقدمي الخدمات السحابية (CSP)

تحدد هذه الفقرة التهديدات التي تؤثر في مقدمي الخدمات السحابية بشكل مباشر. وقد تؤثر هذه التهديدات في قدرة عميل الخدمة السحابية على توفير الخدمات والقيام بأعمال تجارية والاحتفاظ بالعملاء وتجنب الصعوبات القانونية والتنظيمية. كما أن التهديدات التي يتعرض لها عميل معين من عملاء الخدمة السحابية تعتمد على عروض وبيئات الخدمات المحددة الخاصة به.

1.2.7 النفاذ غير المرخص إلى الإدارة

تشمل خدمة الحوسبة السحابية المكونات المتعلقة بالسطوح البينية والبرمجيات التي تتيح لموظفي عميل الخدمة السحابية إدارة جوانب خدمة الحوسبة السحابية التي تقع تحت سيطرة العميل، مثل إضافة حسابات موظفي عميل الخدمة السحابية أو إلغائها، والتوصيل بالمخدِّمات الخاصة بعميل الخدمة السحابية، وإدخال تغييرات على قدرة الخدمة، وتحديث بنود نظام أسماء الميادين (DNS) والمواقع الإلكترونية الخاصة به، وما إلى ذلك. وقد تصبح هذه السطوح البينية الإدارية هدفاً قيماً للمهاجمين الذين ينتحلون شخصيات المسؤولين لدى عميل الخدمة السحابية لمهاجمة مقدم الخدمة السحابية. وبما أن النفاذ إلى خدمات الحوسبة السحابية يجب أن يتوفر لموظفي عميل الخدمة السحابية، فإن حماية هذه الخدمات تصبح مدعاة قلق كبير لأمن الحوسبة السحابية.

2.2.7 التهديدات داخلية المصدر

عندما يتعلق الأمر ببني البشر، يبرز على الدوام خطر قيام الأفراد بالتصرف بطريقة مسببة للأذى أو لا مبالية تعرّض أمن الخدمة للخطر.

فمشاركة موظفي عميل الخدمة السحابية في كلمات السر الخاصة "بمسؤول" الخدمة أو ترك أوراق الاعتماد غير آمنة (مدونة مثلاً على قصاصات ملصقة على الشاشة)، أو وجود مستعملين لا مبالين أو غير مدربين بالقدر الكافي، أو الأفعال الخبيثة التي يقوم بها بعض الموظفين الناقمين، هي أمور تشكل دائماً تهديداً كبيراً لأي عمل تجاري.

ويتعين على عميل الخدمة السحابية بوجه خاص أن ينظر بكل جدية إلى موثوقية موظفيه الخاصين. فعلى الرغم من الفحص الجيد للموظفين، هناك دائماً خطر يتمثل بنجاح أحد الدخلاء في الحصول على مركز بين موظفي مركز البيانات الخاص بعميل الخدمة السحابية. وقد يسعى هذا الدخيل إلى إضعاف عميل الخدمة السحابية نفسه، أو قد ينوي اختراق أنظمة محددة يجري دعمها من أنظمة عميل الخدمة السحابية، ولا سيما إذا كان عميل الخدمة السحابية هذا شركة بارزة أو وكالة حكومية.

8 التحديات الأمنية للحوسبة السحابية

تشمل التحديات الأمنية مصاعب خلاف التهديدات الأمنية الناشئة عن طبيعية خدمات الحوسبة السحابية وبيئتها التشغيلية، بما في ذلك التهديدات "غير المباشرة". ويبرز التهديد غير المباشر حين ينطوي تهديد لأحد المشاركين في خدمة سحابية على تأثيرات سلبية على الآخرين.

وما لم يتم التصدي على نحو سليم للتحديات المحددة في هذه التوصية، فإنها قد تفتح الباب أمام التهديدات. ولا بد من النظر في هذه التهديدات لدى دراسة خدمات الحوسبة السحابية.

1.8 التحديات الأمنية لعملاء الخدمة السحابية (CSC)

تقدم هذه الفقرة وصفاً للتحديات الأمنية المرتبطة بالمصاعب البيئية أو التهديدات غير المباشرة التي قد ينشأ عنها المزيد من التهديدات المباشرة لمصالح عملاء الخدمة السحابية.

1.1.8 غموض المسؤوليات

يستهلك عملاء الخدمة السحابية الموارد المقدمة من خلال فئات خدمات ونماذج نشر مختلفة. وبذلك فإن نظام تكنولوجيا المعلومات والاتصالات القائم على أساس احتياجات العملاء يعتمد على تلك الخدمات. وقد يؤدي أي نقص في وضوح التعريف للمسؤوليات فيما بين عملاء الخدمة السحابية ومقدمي الخدمات السحابية إلى تضارب في المفاهيم وفي عمليات التشغيل. وقد يؤدي وجود أي تعارض في التعاقدات بشأن الخدمات المقدمة إلى نشوء حالة شاذة أو حوادث. وعلى سبيل المثال، فإن المشكلة المتمثلة في تحديد الكيان الذي يشكل مراقب البيانات والآخر الذي يمثل معالج البيانات قد يكتنفها الغموض على المستوى الدولي، حتى وإن تم اختزال الجانب الدولي إلى أدنى طرف من الأطراف الثالثة خارج منطقة محددة مثل الاتحاد الأوروبي.

وبسبب المتطلبات القانونية والتنظيمية، فإن أية شكوك ذات صلة (مثلاً بشأن ما إذا كان عميل الخدمة السحابية أو مقدم الخدمة السحابية هو "مراقب البيانات" أو "معالج البيانات") قد تفضي إلى حالة من الغموض فيما يتعلق بتحديد مجموعة الأنظمة التي يتعين التقيد بها. وإذا ما تباين هذا التفسير ضمن ولايات قضائية مختلفة، فإن عميل الخدمة السحابية أو مقدم الخدمة السحابية سيكتشف أنه يخضع لأنظمة متضاربة بشأن نفس الخدمة أو نفس الجزء من البيانات.

2.1.8 فقدان الثقة

من الصعب أحياناً على عميل الخدمة السحابية أن يدرك مستوى الثقة لدى مقدم الخدمة السحابية بسبب السمات المتعلقة بالصندوق الأسود لخدمة الحوسبة السحابية. وفي حال عدم تواجد السبل للحصول على مستوى الأمن لدى مقدم الخدمة وتقاسمه بطريقة أُضفي عليها الطابع الرسمي، فلن تتوافر لدى عملاء الخدمة السحابية السبل لتقييم مستوى تنفيذ الأمن الذي حققه مقدم الخدمة السحابية. وإن نقصاً كهذا في تقاسم مستوى الأمن فيما يتعلق بمقدم الخدمة السحابية قد يتحول إلى عامل تهديد خطير للأمن بالنسبة لبعض عملاء الخدمة السحابية في سياق استخدامهم لخدمات الحوسبة السحابية.

3.1.8 غياب الإدارة

ينطوي القرار الذي يتخذه عملاء خدمات الحوسبة بشأن ترحيل قسم من نظام تكنولوجيا المعلومات والاتصالات الخاص بهم إلى البنية التحتية للحوسبة السحابية على منح السيطرة الجزئية إلى مقدم الخدمة السحابية. وقد يشكل ذلك تهديداً خطيراً للبيانات الخاصة بعميل الخدمة السحابية، ولا سيما فيما يتعلق بالدور والصلاحية المسندين لمقدم الخدمة. ويؤدي ذلك، مشفوعاً بنقص في الشفافية فيما يتعلق بممارسات مقدمي خدمات الحوسبة السحابية، إلى تشكيل خاطئ، أو يسهم في شن هجوم خبيث من الداخل.

ولدى اعتماد خدمات الحوسبة السحابية، قد يساور بعض عملاء الخدمات السحابية بعض القلق بشأن الافتقار إلى السيطرة على بياناتهم وأصولهم المستضافة لدى مقدمي الخدمات السحابية، وعلى تخزين البيانات، وموثوقية النسخ الاحتياطية للبيانات (قضايا تتعلق بالاحتفاظ بالبيانات)، والتدابير المضادة لخطط الاستمرارية التجارية والتعافي من الأعطال الكبرى، ونحو ذلك.

فعلى سبيل المثال:

- يبدي عميل الخدمة السحابية رغبة في شطب ملف معين لأسباب قانونية، لكن مقدم الخدمة السحابية يحتفظ بنسخة له دون علم عميل الخدمة السحابية بذلك.
- يمنح مقدم الخدمة السحابية مسؤول عميل الخدمة السحابية صلاحيات تتجاوز ما تنص عليه السياسة الخاصة بعميل الخدمة السحابية.
- قد يساور بعض عملاء الخدمة السحابية القلق حيال قيام مقدم الخدمة السحابية بعرض المعطيات على حكومات أجنبية مما قد يؤثر في تقيد عميل الخدمة السحابية بقوانين الخصوصية، مثل توجيهات الاتحاد الأوروبي بشأن حماية البيانات.

4.1.8 فقدان الخصوصية

عندما يمتلك مقدم الخدمة السحابية معلومات خاصة، يبرز احتمال انتهاك الخصوصية مما يتعارض مع أنظمة أو قوانين الخصوصية. ويتضمن ذلك تسرب المعلومات الخاصة، أو معالجة المعلومات الخاصة لأغراض لم يُرخص بها لعميل الخدمة السحابية و/أو صاحب البيانات.

5.1.8 عدم توفّر الخدمة

ليس توفر الخدمة أمراً خاصاً ببيئة الحوسبة السحابية. بيد أنه بسبب مبدأ التصميم الموجه نحو الخدمة، فإن تقديم الخدمات قد يتأثر حين لا تكون خدمات الحوسبة السحابية باتجاه المصدر متوفرة بشكل تام. وعلاوة على ذلك، فإن الاعتماد الدينامي على الحوسبة السحابية يطرح قدراً أكبر من الاحتمالات أمام المهاجم. فهجوم يرمي إلى قطع الخدمة عن خدمة واحدة باتجاه المصدر على سبيل المثال قد يؤثر في العديد من الخدمات باتجاه المقصد في نظام الحوسبة السحابية نفسه.

6.1.8 الحظر الذي يفرضه مقدم الخدمة السحابية

يمكن أن يؤدي ارتفاع مستوى الاعتماد على مقدم واحد للخدمة السحابية إلى زيادة صعوبة استبدال مقدم خدمة سحابية بمقدم آخر لها. وتحدث هذه الحالة حين يعتمد مقدم الخدمة السحابية على مهام أو أنساق غير معيارية ولا يوفر قابلية التشغيل البيني. وقد يمثل ذلك تهديداً أمنياً إذا ما أخفق مقدم الخدمة السحابية الذي يفرض الحظر في التصدي لمواطن الضعف الأمني، مما يجعل عميل الخدمة السحابية معرضاً للخطر وعاجزاً عن الانتقال إلى مقدم آخر من مقدمي الخدمات السحابية.

7.1.8 سوء استعمال الملكية الفكرية

حين يتم تشغيل شفرة عميل الخدمة السحابية أو تخزين أصوله الأخرى من قبل مقدم الخدمة السحابية، فقد تنشأ تحديات تتمثل في احتمال تسرب هذه المواد إلى أطراف ثالثة أو إساءة استعمالها في استخدامات غير مسموحة. وقد يشتمل ذلك على انتهاك لحقوق التأليف والنشر أو إفشاء للأسرار التجارية.

8.1.8 فقدان سلامة البرمجيات

بمجرد تشغيل شفرة عميل الخدمة السحابية في مجال مقدم الخدمة السحابية، يبرز احتمال تحوير الشفرة أو تعرضها للعطب أثناء خروجها عن حيز السيطرة المباشرة لعميل الخدمة السحابية، مما يتسبب في سوء تصرف البرمجيات بطريقة أو بأخرى. ومع أن هذا الاحتمال قائم خارج نطاق سيطرة عميل الخدمة السحابية، فإنه قد يؤثر تأثيراً خطيراً في سمعته وبالتالي في أعماله التجارية.

2.8 التحديات الأمنية لمقدمي الخدمات السحابية (CSP)

تقدم هذه الفقرة وصفاً للتحديات الأمنية المرتبطة بالمصاعب البيئية أو التهديدات غير المباشرة التي قد تفضي إلى نشوء تهديدات مباشرة بصورة أكبر لمصالح مقدم الخدمة السحابية.

1.2.8 غموض المسؤوليات

يمكن تحديد الأدوار المختلفة (مقدم الخدمة السحابية (CSP) وعميل الخدمة السحابية (CSC) والشريك في الخدمة السحابية (CSN)) ضمن إطار نظام الحوسبة السحابية. وأي غموض يكتنف تحديد المسؤوليات المتصلة بقضايا من قبيل امتلاك البيانات أو التحكم بالنفاذ أو صيانة البنية التحتية قد يؤثر في الأعمال التجارية أو المنازعات القانونية (ولا سيما عند التعامل مع أطراف ثالثة، أو حين يكون مقدم الخدمة السحابية هو أيضاً عميلاً للخدمة السحابية أو شريكاً في الخدمة السحابية (CSN)). وتتزايد حدة هذا الغموض حين يشغّل مقدم الخدمة السحابية و/أو يقدم خدمات عبر ولايات قضائية متعددة حيث يُحتمل وجود تعاقدات أو اتفاقات بلغات مختلفة أو بأطرٍ قانونية مختلفة. انظر أيضاً الفقرة 4.2.8 "النزاع القضائي" أدناه.

2.2.8 تقاسم البيئة

تطرح الحوسبة السحابية احتمال تحقيق وفورات في التكاليف من خلال التقاسم المكثّف للموارد الذي يتم على نطاق واسع للغاية. ويعمل هذا الوضع على تعريض الكثير من السطوح البينية الضعيفة. فعلى سبيل المثال، يستهلك عملاء مختلفون للخدمة السحابية الخدمات من الخدمة السحابية نفسها بصورة متزامنة. ونتيجة لذلك، يُحتمل أن يحصل عميل الخدمة السحابية على نفاذ غير مسموح إلى الآلات الافتراضية لشاغلين آخرين، وإلى الحركة في الشبكات، والبيانات الفعلية/المتبقية، ونحو ذلك. وقد يؤدي أي نفاذ غير مسموح أو نفاذ خبيث كهذا إلى أصول عميل آخر من عملاء الخدمات السحابية إلى الإخلال بالسلامة وإمكانية التوفر والسرية.

فعلى سبيل المثال، تتقاسم آلات افتراضية متعددة التي يشترك في استضافتها مخدّم مادي واحد كلاً من وحدة المعالجة المركزية (CPU) وموارد الذاكرة التي يتم تمثيلها الافتراضي من قبل مشرف أعلى. وهذا المثال على التحديات يشمل إخفاق آليات العزل الخاصة بالمشرف الأعلى، مما يجيز النفاذ غير المسموح إلى ذاكرة أو تخزين آلات افتراضية أخرى.

3.2.8 عدم الاتساق والتضارب في آليات الحماية

بالنظر إلى المعمارية اللامركزية للبنية التحتية للحوسبة السحابية، قد تكون آليات الحماية الخاصة بها غير متسقة فيما بين الوحدات الأمنية الموزعة. فنفاذ معين تمنعه وحدة أمنية مثلاً قد تمنحه وحدة أخرى. وقد يتسبب عدم الاتساق هذا في مشكلات لمستخدم مرخّص له، وقد يُستغل من قبل أحد المهاجمين، ما يؤدي بالتالي إلى الإخلال بالسرية والسلامة وإمكانية التوفر.

4.2.8 النزاع القضائي

يمكن نقل البيانات في الخدمة السحابية وتحريكها بين مراكز البيانات، أو حتى عبر الحدود الدولية. وبحسب البلد المضيف، تُدار البيانات من قبل ولايات قضائية مختلفة سارية المفعول. فبعض الولايات القضائية، كالاتحاد الأوروبي على سبيل المثال، تتطلب حمايةً مكثفة للمعلومات المحددة لهوية الشخص (PII) والتي لا يمكن معالجتها في العادة في الأماكن التي لا توفر مستوى كافياً من الحماية المضمونة. وكمثال آخر، قد تتعامل بعض الولايات القضائية مع الاتصالات كخدمة (CaaS) بوصفها خدمة معلومات غير منظمة في حين تتعامل بعض الولايات الأخرى معها كخدمة مهاتفة منظمة. وقد يفضي هذا النزاع القضائي إلى تعقيدات قانونية.

5.2.8 المخاطر التطورية

تتمثل إحدى مزايا الحوسبة السحابية في إرجاء إجراء بعض الخيارات من مرحلة تصميم النظام إلى مرحلة التنفيذ. ويعني ذلك أنه لا يمكن اختيار وتنفيذ بعض مكونات برمجيات النظام التابعة إلا بعد أن يتم تنفيذ المهمة التي تتطلب تلك المكونات. ومع ذلك فإن المنهجية التقليدية لتقييم المخاطر لم تعد تتلاءم مع نظام يتطور بهذا القدر من الدينامية. فأي نظام تمكّن من اجتياز التقييم الأمني أثناء مرحلة التصميم قد تبرز لديه مواطن ضعف وثغرات جديدة أثناء دورة حياته نتيجة التغيرات في مكوّنات البرمجيات.

6.2.8 سوء التحول والتكامل

يتضمن التحوّل إلى خدمة سحابية نقل كميات كبيرة من البيانات وإجراء تغييرات كبرى في التشكيلة (عنونة الشبكات مثلاً). فقد يستدعي تحول قسم من نظام تكنولوجيا المعلومات والاتصالات إلى مقدم خارجي للخدمة السحابية إجراء تغييرات جوهرية في تصميم النظام (مثلاً السياسات المتعلقة بالشبكات والأمن). وقد يسفر سوء التكامل الناجم عن السطوح البينية غير المتوافقة أو الإنفاذ غير المتسق للسياسات عن تأثيرات وظيفية وأخرى غير وظيفية. وعلى سبيل المثال، فإن الآلات الافتراضية التي تعمل خلف جدار الحماية داخل مركز بيانات خاص تتعرض عن طريق الخطأ للإنترنت المفتوحة في الخدمة السحابية لمقدم الخدمات السحابية.

7.2.8 انقطاع الأعمال التجارية

تعمل الحوسبة السحابية على تخصيص الموارد وتقديمها كخدمة. ويتكون النظام الإيكولوجي للحوسبة السحابية من الكثير من الأجزاء المترابطة والتي تعتمد على بعضها البعض. وقد يؤثر انقطاع عمل أي جزء (مثل التعتيم ومنع الخدمة أو التأخر) في توفر خدمة الحوسبة السحابية المرتبط بالفقرة 5.1.8 "عدم توفر الخدمة"، وبالتالي يؤدي إلى انقطاع الأعمال التجارية.

8.2.8 الحظر الذي يفرضه الشريك في الخدمة السحابية

تُبنى منصة مقدم الخدمة السحابية باستخدام مكونات للتجهيزات والبرمجيات مصدرها عدد من المورّدين المختلفين. وقد تشتمل بعض المكونات على ميزات الملكية أو التمديدات الخاصة التي تكون مفيدة لمقدم الخدمة السحابية. بيد أن الاعتماد على ميزات الملكية تلك قد يحد من قدرة مقدم الخدمة السحابية على الانتقال إلى مورّد آخر للمكونات.

ومع أن الحظر يعتبر قضية تجارية، لكنه لا يشكل في حد ذاته تهديداً أمنياً. غير أنه قد يؤدي إلى نشوء شواغل تتعلق بالأمن في بعض الأحيان. ففي حال قيام الشريك في الخدمة السحابية الذي يؤمّن مكوناً من المكونات الأساسية بترك عمله التجاري على سبيل المثال، فقد يعني ذلك عدم توفر المزيد من الرقع البرمجية الأمنية. فعند بروز إمكانية التعرض للخطر في مكون ما، قد يكون التخفيف من حدة المخاطر صعباً للغاية أو باهظ التكاليف.

9.2.8 نقطة ضعف سلسلة التوريد

يُصبح مقدم الخدمة السحابية في خطر إذا ما عملت التجهيزات أو البرمجيات التي سُلّمت إلى المنصة عبر سلسلة التوريد على إضعاف أمن عميل الخدمة السحابية أو مقدم الخدمة السحابية، مثل الإدخال العرضي أو المتعمد لبرمجيات ضارة أو لمواطن ضعف يمكن استغلالها.

والمثال المحدد في هذا الصدد هو ورود شفرة مغلوطة من الشريك في الخدمة السحابية. فهذا التحدي الأمني قائم بالنسبة لشفرة الشريك في الخدمة السحابية المشغلة لدى مقدم الخدمة السحابية، مثلاً لدى قيام العميل بمواجهة نظام التشغيل الخاص بالضيوف (OS) لآلة افتراضية (VM) أو للتطبيقات أو مكونات المنصة أو برمجيات مراجعة/مراقبة الحسابات (مثلاً لشريك يقدم خدمة مراجعة الحسابات).

وهناك مثال آخر في هذا الخصوص، وهو حين يقوم مقدم الخدمة السحابية بتشغيل شفرة مقدمة من الشريك؛ إذ يكون مقدم الخدمة السحابية عرضةً للخطر إذا ما عجز الشريك عن توفير أحدث ما يلزم من مستجدات أمنية في الوقت المناسب.

10.2.8 الاعتماد على البرمجيات

عندما يتم الكشف عن مواطن الضعف، قد يكون من غير الممكن استخدام التحديثات على الفور لأن فعل ذلك قد يعمل على إيقاف عمل مكونات برمجية أخرى (مع أن تلك المكونات قد لا تتطلب تحديثاً لولا ذلك). وينطبق ذلك بوجه خاص إذا كان الاعتماد على البرمجيات قائماً بين مكونات مقدمة من شريك أو أكثر من الشركاء في الخدمة السحابية، بدلاً من مقدمي الخدمات السحابية أنفسهم.

3.8 التحديات الأمنية للشريك في الخدمة السحابية (CSN)

يُنظر في هذه الفقرة في التحديات التي تؤثر بشكل مباشر في الشركاء في الخدمة السحابية. وقد تؤثر هذه التحديات في قدرة الشريك في الخدمة السحابية على النهوض بعمله، وتقاضي الأجر، وحماية ملكيته الفكرية، وتفادي المصاعب القانونية أو التنظيمية. فالتحديات الأمنية بالنسبة لشركاء معينين في الخدمة السحابية تعتمد على الأعمال التجارية أو البيئات الخاصة بهم، مثل التطوير أو التكامل أو المراجعة أو خلاف ذلك.

1.3.8 غموض المسؤوليات

عند تشغيل شفرة في الخدمة تكون مزيجاً من شفرتي مقدم الخدمة السحابية والشريك في الخدمة السحابية، قد لا يتبدى بوضوح بالنسبة لعميل الخدمة السحابية أين تكمن المسؤولية عن التخفيف من حدة الحوادث الأمنية أو معالجتها. وقد يكون من الصعب جداً تحديد الكيان المسؤول عن طريق التحليل التقني. وقد يسفر ذلك عن تبادل الاتهامات بين مقدم الخدمة السحابية والشركاء في الخدمة السحابية بشأن تحديد من هو المخطئ، الأمر الذي قد يفضي إلى المزيد من الخروقات إذا بقيت الأسباب الجذرية غير معروفة.

2.3.8 سوء استعمال الملكية الفكرية

حين يقدم الشركاء شفرات أو أصولاً أخرى إلى مقدم الخدمة السحابية لغرض تنفيذها، فإن التحدي الأمني القائم يتمثل في احتمال تسرب هذه المواد إلى أطراف ثالثة أو إساءة استعمالها في استخدام غير مسموح. وقد يتضمن ذلك انتهاكاً لحقوق التأليف والنشر أو إفشاءً للأسرار التجارية.

3.3.8 فقدان سلامة البرمجيات

بمجرد تشغيل شفرة عميل الخدمة السحابية في مجال مقدم الخدمة السحابية، يبرز احتمال تحوير الشفرة أو تعرضها للعطب أثناء خروجها عن حيز السيطرة المباشرة لعميل الخدمة السحابية، مما يتسبب في سوء تصرف البرمجيات بطريقة أو بأخرى. ومع أن هذا الاحتمال قائم خارج نطاق سيطرة عميل الخدمة السحابية، فإنه قد يؤثر تأثيراً خطيراً في سمعته وبالتالي في أعماله التجارية.

9 قدرات الأمن في الحوسبة السحابية

تحدد هذه التوصية قدرات الأمن التالية لمواجهة التهديدات والتحديات المحددة في أمن الحوسبة السحابية. أما المعلمات المتعلقة بقدرات الأمن هذه، مثل مدة الاستجابة للحوادث، فيمكن أن ينص عليها الاتفاق على مستوى الخدمة (SLA) الأمنية.

1.9 نموذج الثقة

يعتبر نموذج الثقة المشترك ضرورياً لأي نظام يتعاون فيه عدد من مقدمي الخدمات لتوفير خدمة جديرة بالثقة.

ونظراً إلى الطابع متعدد أصحاب المصلحة وذي الدرجة العالية من التوزيع للحوسبة السحابية، يتعين على بيئة الحوسبة السحابية إدراج نموذج شامل للثقة. ويتيح نموذج الثقة هذا إيجاد جزر و/أو اتحادات من الكيانات الموثوقة بحيث تتمكن العناصر المتفرقة للنظام من استيقان هوية الكيانات والمكونات الأخرى والحقوق المسموحة. ويستند كلّ من جزر أو اتحادات الثقة إلى واحدة أو أكثر من السلطات الموثوقة (مثلاً سلطة إصدار شهادات البنية التحتية للمفاتيح العمومية (PKI)).

ويوجد حالياً عدة نماذج للثقة لأغراض الحوسبة السحابية وغير السحابية على السواء. أما نموذج الثقة المحدد المقرر اعتماده فيقع خارج نطاق هذه التوصية.

2.9 إدارة خدمات الهوية والنفاذ (IAM)، والاستيقان والترخيص ومراجعة العمليات

يشترك في خدمات الحوسبة السحابية عدد من المسؤولين والمستعملين، ويتوفر النفاذ إلى خدمات الحوسبة السحابية هذه واستعمالها داخلياً (CSP) وخارجياً (CSC). وتدعو الحاجة إلى إدارة الهويات ليس فقط من أجل حمايتها بل لتسهيل عمليات إدارة النفاذ والاستيقان والترخيص ومراجعة العمليات في هذه البنية التحتية الدينامية والمفتوحة للخدمة السحابية.

وتحتاج إدارة خدمات الهوية والنفاذ إلى واحد أو أكثر من نماذج الثقة المشتركة (الفقرة 1.9) من أجل استيقان الهويات، كما يحتاج إليها المطوّرون والمشرفون الأعلى وغيرهم من مكونات النظام من أجل استيقان مكونات النظام من قبيل وحدات البرمجيات أو التطبيقات أو مجموعات البيانات التي جرى تنزيلها.

وتساهم إدارة خدمات الهوية والنفاذ في ضمان سرية الخدمات والموارد وسلامتها وتوفرها، وتعتبر بالتالي أساسية في الحوسبة السحابية.

وعلاوة على ذلك، فقد تمكن إدارة خدمات الهوية والنفاذ من إنشاء اتحاد بهوية واحدة وتوقيع دخول واحد إلى الخدمات السحابية باستخدام آليات استيقان مختلفة أو موزعة في مجالات أمنية مختلفة.

وتوفر مراجعة العمليات الحماية من التنصل، وتسمح بإجراء تحليل جنائي بعد حادث أمني، وتقوم بردع الهجمات (الاقتحامية أو الداخلية المصدر على السواء). ومع أن مراجعة العمليات تنطوي على أكثر من مجرد عملية تسجيل، إلا أنها تشمل أيضاً المراقبة الفاعلة بهدف التأشير على الأنشطة المريبة.

3.9 الأمن المادي

الأمن المادي هو أمن يتعين تحقيقه. ويكون النفاذ إلى الأماكن التي تحتوي على تجهيزات عميل الخدمة السحابية محصوراً بالأشخاص المرخص لهم وفقط في المجالات التي تلزم مباشرة لتأدية وظائف عملهم؛ وهذا الأمر يشكل جزءاً من عملية إدارة خدمات الهوية والنفاذ. ومع ذلك يعتمد مدى الأمن المادي على قيمة البيانات ومدى النفاذ المسموح به للعملاء المتعددين.

4.9 أمن السطوح البينية

تؤمن هذه القدرة بقاء السطوح البينية مفتوحة لعملاء الخدمة السحابية و/أو مقدمي الخدمات السحابية الآخرين المتعاقدين الذين يتم من خلالهم توفير الأنواع المختلفة من خدمات الحوسبة السحابية، كما تؤمن الاتصالات القائمة على هذه السطوح البينية. وتشمل الآليات المتاحة لضمان أمن السطوح البينية على سبيل المثال لا الحصر الاستيقان أحادي الجانب/المتبادل، وسلامة المجموع التدقيقي، والتجفير من طرف إلى طرف، والتوقيع الرقمي وما إلى ذلك.

5.9 أمن التمثيل الافتراضي للحوسبة

يشير أمن التمثيل الافتراضي للحوسبة إلى أمن بيئة التمثيل الافتراضي للحوسبة بأكملها. وهو يحمي المشرف الأعلى من الهجمات، ويحمي المنصة المضيفة من التهديدات الناجمة عن بيئة التمثيل الافتراضي للحوسبة، ويبقي الآلات الافتراضية آمنة طوال دورة الحياة. وتتيح هذه القدرة تحديداً إمكانية عزل الآلة الافتراضية، وتحمي صور الآلة الافتراضية والحالات أو العمليات المعلقة للآلة الافتراضية التي تكون مختزنة وأثناء عملية الانتقال.

وبالنسبة لعميل الخدمة السحابية، يوفر المشرف الأعلى عادة الحماية للآلات الافتراضية المضيفة، وذلك مثلاً بتوفير معالجة مضادة للفيروسات وللرسائل الاقتحامية داخل المشرفين الأعلى، بحيث لا تحتاج الآلات الافتراضية إلى تنفيذ هذه الوظائف بشكل مستقل. وتكون تشكيلة المشرف الأعلى عادة بأدنى مجموعة من الخدمات. وعادة تكون السطوح البينية وسطوح برمجة التطبيقات مغلقة (API) والمكونات غير المتصلة بالخدمة معطلة.

وتشمل الآلات الافتراضية التي تغطيها هذه القدرة تلك التي يستحدثها عميل الخدمة السحابية في البنية التحتية كخدمة (IaaS)، إلى جانب أي آلات افتراضية تستحدثها البرمجيات كخدمة (SaaS) والمنصات كخدمة (PaaS). وتكون الآلات الافتراضية عادة معزولة بشكل جيد عند تقاسم الذاكرة ووحدة المعالجة المركزية (CPU) وقدرات التخزين. وتتسم الآلات الافتراضية بقدرات أمن أصيلة ودرجة وعي خاص بالسياسات (كنظام التشغيل الخاص بالضيوف مثلاً).

6.9 أمن الشبكات

يتيح أمن الشبكات في بيئة الحوسبة السحابية عزل كل من الشبكات المادية والافتراضية ويؤمن الاتصالات بين جميع المشاركين. كما يتيح تجزئة الميدان الأمني للشبكات والتحكم في النفاذ على حدود الشبكات (كجدران الحماية مثلاً)، وكشف الاقتحام ومنعه، وفصل حركات الشبكات استناداً إلى سياسات الأمن، كما يحمي الشبكة من الهجمات في البيئتين المادية والافتراضية على السواء.

7.9 عزل البيانات وحمايتها وحماية الخصوصية

تعالج هذه القدرة القضايا العامة لحماية البيانات التي قد يترتب عليها عادة آثار قانونية.

- عزل البيانات

يُمنع الشاغل في إطار الحوسبة السحابية من النفاذ إلى بيانات تخص شاغلاً آخر، حتى وإن كانت البيانات مجفّرة، إلا إذا كان النفاذ مسموحاً صراحة. وقد يتحقق عزل البيانات بطريقة منطقية أو مادية تبعاً لدقة العزل المطلوب والنشر المحدد لبرمجيات الحوسبة السحابية وتجهيزاتها.

الملاحظة 1– يحدث العزل في الحوسبة السحابية على مستوى الشاغل. وقد يكون لأحد عملاء الحوسبة السحابية عدة شاغلين في الخدمة السحابية، وذلك مثلاً لفصل الكيانات التابعة أو الشعب أو الوحدات التجارية المختلفة عن بعضها البعض.

- حماية البيانات

تضمن حماية البيانات أن تكون بيانات عميل الخدمة السحابية والبيانات المشتقة منها والمحتفظ بها في بيئة الحوسبة السحابية محمية بالشكل الصحيح بحيث لا يمكن النفاذ إليها أو تغييرها إلا على النحو الذي سمح به عميل الخدمة السحابية (أو وفقاً لقانون ساري المفعول). وقد تشمل هذه الحماية توليفة من قوائم التحكم في النفاذ، وتدقيق السلامة، وتصحيح الأخطاء/استعادة البيانات، والتجفير، وغير ذلك من الآليات المناسبة.

وعندما يوفر مقدم الخدمة السحابية لعملاء الخدمة السحابية إمكانية تجفير الخزن، فقد تكون هذه الوظيفة تجفيراً من جانب العميل (مثلاً ضمن تطبيق خاص بعميل الخدمة السحابية) أو تجفيراً من جانب المخدّم.

- حماية الخصوصية

يمكن أن تشمل حماية الخصوصية المعلومات المحددة لهوية الشخص والبيانات السرية للشركات. وقد يخضع جمع المعلومات الخاصة ومعالجتها وتخزينها وإتلافها إلى اللوائح أو القوانين المتعلقة بالخصوصية. وينطبق هذا التقييد على كل من مقدمي الخدمات السحابية وعملاء الخدمة السحابية التابعين لهم، إذ يتعين مثلاً على عميل الخدمة السحابية أن يكون قادراً على حذف جدول بيانات يحتوي على معلومات خاصة حتى ولو كان مقدم الخدمة السحابية على غير علم بمحتويات الجدول. وقد يحتاج مقدمو الخدمات السحابية أيضاً إلى دعم عملية المعالجة، كالبحث مثلاً في بيانات عملاء الخدمة السحابية بشكليها المحوّل أو المجفّر.

وتمتد حماية الخصوصية لتشمل المعلومات الخاصة التي يمكن رصدها أو استخلاصها من أنشطة عميل الخدمة السحابية، مثل الاتجاهات التجارية، والعلاقات أو الاتصالات مع باقي الأطراف، ومستويات النشاط وأنماطه، وما إلى ذلك.

كما أن حماية الخصوصية مسؤولة عن التأكد من أن جميع المعلومات الخاصة (بما فيها المعلومات المرصودة أو المستخلصة) لا تستعمل إلا للأغراض المتفق عليها بين عميل الخدمة السحابية ومقدم الخدمة السحابية.

وقد يسهم تقييم المخاطر المتعلقة بالمعلومات الخاصة (يشار إليه باسم "تقييم مخاطر الخصوصية") بمساعدة مقدم الخدمة السحابية في تحديد المخاطر الخاصة بانتهاك الخصوصية التي تدخل في إحدى العمليات المتوخاة. ويتعين على مقدم الخدمة السحابية أن يحدد وينفذ القدرات اللازمة للتصدي لمخاطر الخصوصية التي حددها تقييم مخاطر المعلومات الخاصة ومعالجتها.

الملاحظة 2– في بعض الولايات القضائية، يُعامل الأفراد الطبيعيون (أي المستعملون من البشر) بشكل منفصل عن مستخدميهم لأغراض الخصوصية. وفي مثل تلك الظروف تكون خصوصية مستعمل الخدمة السحابية (CSU) محمية بالشكل الصحيح بالإضافة إلى عميل الخدمة السحابية (CSC) أو شاغل الخدمة السحابية.

8.9 التنسيق الأمني

بما أن خدمات الحوسبة السحابية المختلفة تقتضي تنفيذ وسائل تحكم أمنية مختلفة، فإن هذه القدرة الأمنية تنسق بين آليات الأمن المتباينة لتفادي أوجه التضارب في الحماية.

ويؤدي الأطراف أدواراً مختلفة في النظام الإيكولوجي للحوسبة السحابية، حيث يكون لمقدم الخدمة السحابية وعميل الخدمة السحابية والشريك في الخدمة السحابية درجات مختلفة من التحكم في الموارد والخدمات المادية أو الافتراضية، بما في ذلك التحكم في الأمن.

وتتوفر لكل طرف آليات أمنية متنوعة، بما فيها عزل المشرفين الأعلى، وإدارة خدمات الهوية والنفاذ، وحماية الشبكات، وما إلى ذلك.

ومن أهداف الحوسبة السحابية تمكين مجموعة من هذه الأطراف المختلفة من العمل معاً وبشكل تعاوني على تصميم وبناء ونشر وتشغيل مختلف الموارد المادية وذات التمثيل الافتراضي. لذلك يتعين على مقدم الخدمة السحابية أن يكون قادراً على التنسيق بين مختلف الآليات الأمنية عبر الأطراف المختلفة. ويعتمد التنسيق الأمني على قابلية التشغيل البيني وتناسق الآليات الأمنية المتنوعة.

9.9 الأمن التشغيلي

توفر هذه القدرة حماية أمنية لعمليات التشغيل والصيانة اليومية لخدمات الحوسبة السحابية وبنيتها التحتية.

وتتضمن القدرة الأمنية التشغيلية هذه ما يلي:

- تحديد مجموعات من سياسات الأمن وأنشطة الأمن مثل إدارة التشكيلات وتحديث الرقع البرمجية وتقييم الأمن والاستجابة إلى الحوادث (انظر أيضاً الفقرة 10.9 "إدارة الحوادث")، والتأكد من أن هذه التدابير الأمنية تطبق على النحو الصحيح للوفاء بمتطلبات القوانين والعقود السارية بما فيها أي اتفاق أمني على مستوى الخدمة.
- مراقبة التدابير الأمنية لمقدم الخدمة السحابية وفعاليتها وتقديم تقارير مناسبة إلى عملاء الخدمة السحابية المتأثرين بها وإلى المراجعين المعتمدين من أطراف ثالثة (الذين يقومون بدور الشريك في الخدمة السحابية)، ما يمكّن عميل الخدمة السحابية من التأكد من أن مقدم الخدمة السحابية يقدم خدماته وفقاً للالتزامات المنصوص عليها في الاتفاق الأمني على مستوى الخدمة.

وفي الحالة التي تتغير فيها التدابير الأمنية لمقدمي الخدمات السحابية أو فعالية هذه التدابير، يتم تنبيه جميع مقدمي الخدمة السحابية وعملاء الخدمة السحابية في اتجاه المقصد بشأن هذه التغييرات.

وتمكن هذه التقارير والتنبيهات عملاء الخدمة السحابية المرخص لهم من رؤية الحوادث المناسبة ومعلومات المراجعة وبيانات التشكيلات المتعلقة بخدمات الحوسبة السحابية الخاصة بهم.

10.9 إدارة الحوادث

تنص إدارة الحوادث على مراقبة الحوادث والتنبؤ بها والتحذير منها والاستجابة لها. والمراقبة المستمرة ضرورية (مثلاً مراقبة الأداء في الوقت الفعلي لمنصة التمثيل الافتراضي والآلة الافتراضية) لمعرفة ما إذا كانت الخدمة السحابية تعمل على النحو المتوقع على كامل البنية التحتية. ومن شأن ذلك أن يمكّن الأنظمة من معرفة الوضع الأمني للخدمة، وتحديد الظروف غير الطبيعية، وتوفير إنذار مبكر بالحمولات الزائدة للنظام الأمني والخروقات وانقطاع الخدمة وما إلى ذلك. وبعد حصول الحوادث الأمنية، يتم تحديد المشكلة والاستجابة للحادث بسرعة سواء بطريقة أوتوماتية أو بتدخل المسؤول البشري. أما الحوادث الوثيقة الصلة فيتم تسجيلها وتحليلها لمعرفة الأنماط الأساسية المحتملة للتمكن من معالجتها بشكل استباقي.

11.9 التعافي من الأعطال الكبرى

يمثل التعافي من الأعطال الكبرى القدرة على الاستجابة إلى الكوارث الفادحة واستعادة الحالة المأمونة واستئناف العمليات الطبيعية بأسرع وقت ممكن. وتوفر هذه القدرة استمرار الخدمة المقدمة بحد أدنى من الانقطاع.

12.9 تقييم أمن الخدمات ومراجعته

تسمح هذه القدرة بإجراء تقييم أمني لخدمات الحوسبة السحابية. وتمكن الطرف المرخّص له بالتحقق من أن الخدمة السحابية تمتثل لمتطلبات الأمن المعمول بها. ويمكن إجراء التقييم الأمني أو المراجعة الأمنية بواسطة عميل الخدمة السحابية أو مقدم الخدمة السحابية أو طرف ثالث (الشريك في الخدمة السحابية (CSN))، كما يمكن اعتماد شهادات أمنية بواسطة طرف ثالث مرخّص له (CSN).

وتنفذ معايير الأمن المناسبة بحيث توفر تفاهماً متبادلاً للمستوى الأمني بين عميل الخدمة السحابية ومقدم الخدمة السحابية.

وقد يكون لكل عميل من عملاء الخدمة السحابية أو لكل خدمة من خدماته المستوى الأمني المتعلق بأدوات التحكم في الأمن الخاصة بمقدمي الخدمات السحابية وفعاليتها. وتساعد المستويات الأمنية المعلنة لمقدمي الخدمات السحابية وخدماتهم في تيسير المقارنة بين مقدمي الخدمات السحابية وخدمات الحوسبة السحابية واختيار الأنسب من بينها. وقد يتم استخدام أطراف ثالثة مستقلة لتوفير تقييم موثوق ومستقل وحيادي للمستوى الأمني.

ولتفادي قيام مقدّم الخدمة السحابية بإجراء مراجعة أمنية مستقلة لكل عميل من عملاء الخدمة السحابية، يمكن إعادة استعمال نتائج المراجعة المشتركة بطريقة مناسبة. ويمكن لمقدم الخدمة السحابية الذي يغطي مجموعة كبيرة من خدمات الحوسبة السحابية إجراء مراجعة أمنية لكل خدمة سحابية على حدة. وقد يوفر مقدم الخدمة السحابية النتائج المناسبة المتعلقة بمراجعة جميع خدمات الحوسبة السحابية أو جزء منها إلى أحد عملاء الحوسبة السحابية المرخص لهم (كالعميل المحتمل مثلاً)، وإلى بعض مقدمي الخدمات السحابية والشركاء في الخدمة السحابية (كالمراجع المعتمد من طرف ثالث مثلاً).

أما بالنسبة لسلسلة خدمات الحوسبة السحابية، فإن نتائج المراجعة الأمنية لمقدم الخدمة في اتجاه المقصد تتضمن نتائج المراجعة ذات الصلة لمقدمي الخدمات في اتجاه المصدر.

13.9 قابلية التشغيل البيني وقابلية النقل وقابلية الرجوع

تمكن هذه القدرة من تعايش المكونات المتباينة والتعاون فيما بينها (قابلية التشغيل البيني)، وتمكن عملاء الخدمة السحابية من استبدال مقدم خدمة سحابية بمقدم آخر لها عند الاقتضاء (قابلية النقل)، كما تمكن عملاء الخدمة السحابية من إعادة نظام تكنولوجيا المعلومات والاتصالات الخاص بهم من بيئة سحابية إلى بنية تحتية غير سحابية لتكنولوجيا المعلومات والاتصالات (قابلية الرجوع). وتتيح قابلية الرجوع هذه أيضاً "الحق في النسيان" إذا تطلبت القوانين أو اللوائح الوطنية ذلك.

الملاحظة 1– هذه القدرة مسؤولة فقط عن قابلية التشغيل البيني وقابلية النقل للوظائف الأمنية في الحوسبة السحابية، وليس عن البيانات الفعلية أو البيانات الوصفية أو أنساق الرسائل التي تتولى القيام بها وظائف أخرى في منصة الحوسبة السحابية. وعلى سبيل المثال، يمكن لهذه القدرة أن توفر تجفيراً انتقالياً وإدارة للمفاتيح ومعلومات عن الهوية تسمح بنقل البيانات وعناصر المحتوى الأخرى بين نظامي تجفير مختلفين من دون تعرض النظام (النظامين) أو البيانات العابرة للتهديدات.

الملاحظة 2– لم يتم بعد تعريف "الحق في النسيان" بوضوح ويمكن أن يتعارض في بعض الحالات مع الشروط التنظيمية التي تقضي بالاحتفاظ ببعض البيانات لفترة زمنية دنيا، مثل تسجيلات المكالمات والمعلومات المتعلقة بالتوصيل. لذلك قد يكون من الضروري الاحتفاظ بالمفاتيح ذات الصلة أو بالمعلومات الأمنية الأخرى للفترة الزمنية ذاتها.

14.9 أمن سلسلة التوريد

يستعمل مقدم الخدمة السحابية عدداً من الموردين لبناء خدماته. ويكون بعض هؤلاء الموردين من المشاركين في الصناعة السحابية مثل الشريك في الخدمة السحابية، بينما يكون بعضهم الآخر من الموردين التقليديين لتجهيزات وخدمات تكنولوجيا المعلومات (IT)، مثل صانعي التجهيزات ممن لا يمتون بصلة مباشرة إلى الحوسبة السحابية. وتتيح هذه القدرة إرساء علاقة ثقة بين مقدم الخدمة السحابية وجميع المشاركين في سلسلة التوريد بواسطة أنشطة أمنية. وتشمل أنشطة أمن سلسلة التوريد هذه تحديد وتجميع المعلومات عن المكونات والخدمات التي حاز عليها مقدمو الخدمات السحابية والتي تستخدم لتوفير خدمات الحوسبة السحابية وإنفاذ سياسات أمن سلسلة التوريد.

وعلى سبيل المثال، يمكن أن تشمل أنشطة الأمن في سلسلة التوريد ما يلي:

- تأكيد المعلومات الأساسية عن المشاركين في سلسلة التوريد؛

- التحقق من صلاحية التجهيزات والبرمجيات والخدمات التي يستخدمها مقدم الخدمة السحابية؛
- فحص التجهيزات والبرمجيات التي يقتنيها مقدم الخدمة السحابية للتأكد من عدم التلاعب بها أثناء العبور؛
- توفير آليات للتحقق من منشأ برمجيات الخدمة السحابية، مثلاً الشفرة التي يعطيها الشريك في الخدمة السحابية. وعند الاقتضاء يوفر الشركاء في الخدمة السحابية والعملاء المستضافين من قبلهم عملية التحقق من سلامة المكونة البرمجية الخاصة بالشركاء في الخدمة السحابية للتأكد من أنها مطابقة للشكل الذي قُدّمت به وأنها لم تعدل أو يتم المساس بها. وقد يطلب بعض الشركاء في الخدمة السحابية وسائل للتحقق من ذلك بأنفسهم وبشكل مباشر.

وتستمر هذه القدرة بتغطية التطورات الجارية للنظام وتحديثاته.

10 منهجية إطارية

يقصد بوضع إطار أمني للحوسبة السحابية فهم التهديدات والتحديات القائمة كما تم بحثها في الفقرتين 7 و8، وذلك لأنه يتعين اختيار الخدمة السحابية إلى جانب العمل التجاري والمتطلبات التكنولوجية والتنظيمية معاً من أجل تحديد أدوات التحكم والسياسات والإجراءات الأمنية اللازمة للخدمة السحابية المعينة. ثم تستعمل القدرات الواردة في الفقرة 9 للتصدي لهذه التهديدات والتحديات والتخفيف من حدتها من أجل وضع أدوات التحكم والسياسات والإجراءات الأمنية للخدمة السحابية المحددة المختارة. وتركز هذه التوصية على الحاجات الأمنية لبيئة الحوسبة السحابية، والتهديدات والتحديات التي يطرحها وجود بيئة حسابية تقليدية ضمن بيئة الحوسبة السحابية، وبالتالي المعايير وأفضل الممارسات التي تحددها دوائر الصناعة ويتعين التقيد بها بالإضافة إلى هذه التوصية.

وينبغي التقيّد بالمنهجية الواردة هنا من أجل إيجاد إطار يحدد أدوات التحكم الأمنية والسياسات والإجراءات اللازمة لخدمة معينة في الحوسبة السحابية. ومن غير الممكن توفير إطار معياري وحيد لجميع خدمات الحوسبة السحابية، لأنها تتغير بدرجة كبيرة في نماذج الأعمال والخدمات المقدمة وخيارات التنفيذ:

- الخطوة 1: استعِن بالفقرتين 7 و8 لتحديد التهديدات الأمنية والتبعات الأمنية للتحديات في خدمة الحوسبة السحابية المعنية.
- الخطوة 2: استعِن بالفقرة 9 لتحديد القدرات الأمنية الرفيعة المستوى اللازمة، استناداً للتهديدات والتحديات المحددة، التي قد تخفف من حدة التهديدات الأمنية وتتصدى للتحديات الأمنية.
- الخطوة 3: استخلص أدوات التحكم والسياسات والإجراءات الأمنية التي يمكن أن توفر القدرات الأمنية اللازمة بالاستناد إلى القدرات الأمنية المحددة.

ملاحظة – يتعين على عميل الخدمة السحابية ومقدم الخدمة السحابية تحديد مجموعة من المتطلبات المناسبة فيما يتعلق بالقدرات الأمنية باستخدام المعايير الملائمة. ويستند هذا التحديد إلى تقييم المخاطر.

وينبغي مراجعة كل تهديد أو تحدّ للتعرف إلى التهديدات الأمنية والتحديات ذات الصلة بالخدمة السحابية المعنية. وأبسط نهج لذلك يتمثل في جدول يشار فيه إلى التهديد أو التحدي بالحرف Y.

وكمثال على استخدام هذا النهج، فعندما يوفر مقدم الخدمة السحابية خدمة تخزين الملفات للمستعملين الأفراد، فإنه يرغب في فهم التهديدات والتحديات الأمنية التي تهم المستعملين بالدرجة الأساسية، ويجري تحليلاً للتهديدات والتحديات الأمنية التي يتعين على مقدم الخدمة السحابية التصدي لها. ويوضح الجدول 1 هذا النهج.

الجدول 1 – مثال على الخطوة 1 في تحليل الإطار الأمني لتخزين الملفات كخدمة

مجال التحليل	التهديد أو التحدي النوعي	هل ينطبق ذلك على الخدمة؟
الفقرة 1.7 التهديدات الأمنية لعملاء الخدمة السحابية (CSC)	الفقرة 1.1.7 فقدان البيانات وتسربها	Y
	الفقرة 2.1.7 النفاذ غير الآمن للخدمات	Y
	الفقرة 3.1.7 التهديدات داخلية المصدر	
الفقرة 2.7 التهديدات الأمنية لمقدمي الخدمات السحابية (CSP)	الفقرة 1.2.7 نفاذ إدارة غير مخولة	Y
	الفقرة 2.2.7 التهديدات داخلية المصدر	Y
الفقرة 1.8 التحديات الأمنية لعملاء الخدمة السحابية (CSC)	الفقرة 1.1.8 غموض المسؤوليات	Y
	الفقرة 2.1.8 فقدان الثقة	Y
	الفقرة 3.1.8 غياب الإدارة	Y
	الفقرة 4.1.8 فقدان الخصوصية	Y
	الفقرة 5.1.8 عدم توفر الخدمات	Y
	الفقرة 6.1.8 الحظر الذي يفرضه مقدم الخدمة السحابية	Y
	الفقرة 7.1.8 سوء استعمال الملكية الفكرية	
	الفقرة 8.1.8 فقدان سلامة البرمجيات	
الفقرة 2.8 التحديات الأمنية لمقدمي الخدمات السحابية (CSP)	الفقرة 1.2.8 غموض المسؤوليات	Y
	الفقرة 2.2.8 تقاسم البيئة	Y
	الفقرة 3.2.8 عدم الاتساق والتضارب في آليات الحماية	Y
	الفقرة 4.2.8 النزاع القضائي	Y
	الفقرة 5.2.8 المخاطر التطورية	
	الفقرة 6.2.8 سوء التحول والتكامل	Y
	الفقرة 7.2.8 انقطاع الأعمال التجارية	Y
	الفقرة 8.2.8 الحظر الذي يفرضه الشريك في الخدمة السحابية	
	الفقرة 9.2.8 نقطة ضعف سلسلة التوريد	Y
	الفقرة 10.2.8 الاعتماد على البرمجيات	
الفقرة 3.8 التحديات الأمنية للشركاء في الخدمة السحابية (CSN)	الفقرة 1.3.8 غموض المسؤوليات	
	الفقرة 2.3.8 سوء استعمال الملكية الفكرية	
	الفقرة 3.3.8 فقدان سلامة البرمجيات	

وبمجرد التعرف إلى التهديدات والتحديات، يصبح بالإمكان تحديد القدرات الأمنية التي يمكنها أن تخفف من حدة تلك التهديدات وتتصدى لتلك التحديات. ويورد الجدول I-1 مثالاً على التقابل بين التهديدات والتحديات الأمنية من جهة والقدرات الأمنية من جهة ثانية. ويشير الحرف Y في الخلية الواقعة عند التقاء أعمدة وصفوف الجدول بأن تهديداً أو تحدياً أمنياً معيناً قد تم التصدي له بواسطة القدرة الأمنية المقابلة. وتظهر في هذا الجدول جميع التهديدات والتحديات والقدرات الأمنية المقابلة لها.

وبمجرد التعرف إلى القدرات المطلوبة، يصبح بالإمكان تحديد أدوات التحكم والسياسات والإجراءات الأمنية التي تحتاج إليها. ومن الأمثلة على أدوات التحكم اللازمة "الأمن التشغيلي" (الفقرة 12 في [b-ISO/IEC 27002]) و"إدارة حوادث أمن المعلومات" (الفقرة 16 في [b-ISO/IEC 27002])، ويمكن استخلاصهما من القدرات المحددة في الفقرتين 9.9 و10.9 على التوالي.

وقد يكون للخدمة السحابية سلسلة توريد مؤلفة من عدد من مقدمي الخدمات السحابية. ويمكن للشركات المشاركة في سلسلة التوريد هذه الرجوع إلى معايير الاتحاد الدولي للاتصالات والمعايير الصناعية المتعلقة بموضوع أمن سلسلة التوريد (مثلاً [b-ISO/IEC 28000]). ويتعين على كل عميل من عملاء الخدمة السحابية أن يحدد مسؤوليته في سلسلة خدمات الحوسبة السحابية وأن يضع أدوات التحكم والسياسات والإجراءات الأمنية الخاصة به استناداً إلى القدرات الأمنية المستخلصة في هذا النهج الثلاثي الخطوات. ولتوفير أمن متسق لعملاء الخدمة السحابية، قد يتعين على مقدم الخدمة السحابية في اتجاه المصدر أن يتفاوض مع مقدمي الخدمات السحابية التابعين له في اتجاه المقصد بشأن القدرات الأمنية بالاستناد إلى مسؤولياتهم الأمنية. وعند الاقتضاء، يتعين على عملاء الخدمة السحابية التقيد بهذا الإجراء الثلاثي الخطوات أيضاً.

وبالإضافة إلى ذلك، ينبغي تنفيذ الإجراء الثلاثي الخطوات الوارد أعلاه بشكل دوري أو عند الاقتضاء (مثلاً عندما يحدث خرق أمني خطير أو عندما يغيّر عميل الخدمة السحابية مقدم الخدمة السحابية الخاص به في اتجاه المصدر).

التذييل I

جدول التقابل بين التهديدات والتحديات الأمنية للحوسبة السحابية والقدرات الأمنية

(لا يشكل هذا التذييل جزءاً أساسياً من هذه التوصية)

يظهر الجدول 1.I تقابلاً بين التهديدات والتحديات الأمنية للحوسبة السحابية وبين بعض القدرات الأمنية الممكنة.

يشير الحرف Y في الخانات الواقعة عند التقاء أعمدة وصفوف الجدول إلى أن تهديداً وتحدياً أمنياً محدداً قد تم التصدي له بواسطة القدرة الأمنية المقابلة.

الجدول 1.I – التقابل بين التهديدات والتحديات الأمنية للحوسبة السحابية والقدرات الأمنية

			الفقرة 9 قدرات أمن الحوسبة السحابية												
			الفقرة 1.9 نموذج الثقة	**الفقرة 2.9 إدارة خدمات الهوية والنفاذ (IAM)، والاستيقان والترخيص ومراجعة العمليات**	**الفقرة 3.9 الأمن المادي**	**الفقرة 4.9 أمن السطوح البينية**	**الفقرة 5.9 أمن المثيل الافتراضي للحوسبة**	**الفقرة 6.9 أمن الشبكات**	**الفقرة 7.9 عزل البيانات وحمايتها وحماية الخصوصية**	**الفقرة 8.9 التنسيق الأمني**	**الفقرة 9.9 الأمن التشغيلي**	**الفقرة 10.9 إدارة الحوادث**	**الفقرة 11.9 التعافي من الأعطال الكبرى**	**الفقرة 12.9 تقييم أمن الخدمات ومراجعته**	**الفقرة 13.9 قابلية التشغيل البيني وقابلية النقل وقابلية الرجوع**	**الفقرة 14.9 أمن سلسلة التوريد**
الفقرة 7 التهديدات الأمنية للحوسبة السحابية	الفقرة 1.7 التحديات الأمنية لعملاء الخدمة السحابية (CSC)	الفقرة 1.1.7 فقدان البيانات وتسربها	Y	Y	Y				Y				Y		
		الفقرة 2.1.7 النفاذ غير الآمن للخدمات	Y	Y		Y	Y	Y							
		الفقرة 3.1.7 التهديدات داخلية المصدر		Y	Y									Y	
	الفقرة 2.7 التهديدات الأمنية لمقدمي الخدمات السحابية (CSP)	الفقرة 1.2.7 نفاذ إدارة غير مخولة	Y	Y	Y	Y									
		الفقرة 2.2.7 التهديدات داخلية المصدر		Y	Y									Y	

الجدول 1.I – التقابل بين التهديدات والتحديات الأمنية للحوسبة السحابية والقدرات الأمنية

			الفقرة 9 قدرات أمن الحوسبة السحابية											
			الفقرة 1.9 نموذج الثقة	الفقرة 2.9 إدارة خدمات الهوية والنفاذ (IAM)، والاستيقان والترخيص ومراجعة العمليات	الفقرة 3.9 الأمن المادي	الفقرة 4.9 أمن السطوح البينية	الفقرة 5.9 أمن المثيل الافتراضي للحوسبة	الفقرة 6.9 أمن الشبكات	الفقرة 7.9 عزل البيانات وحمايتها وحماية الخصوصية	الفقرة 8.9 التنسيق الأمني	الفقرة 9.9 الأمن التشغيلي	الفقرة 10.9 إدارة الحوادث	الفقرة 11.9 التعافي من الأعطال الكبرى	الفقرة 12.9 تقييم أمن الخدمات ومراجعته	الفقرة 13.9 قابلية التشغيل البيني وقابلية النقل وقابلية الرجوع	الفقرة 14.9 أمن سلسلة التوريد
الفقرة 8 التحديات الأمنية للحوسبة السحابية	الفقرة 1.8 التحديات الأمنية لعملاء الخدمات السحابية (CSC)	الفقرة 1.1.8 غموض المسؤوليات		Y							Y					
		الفقرة 2.1.8 فقدان الثقة	Y											Y		
		الفقرة 3.1.8 غياب الإدارة		Y	Y				Y		Y	Y	Y	Y		
		الفقرة 4.1.8 فقدان الخصوصية		Y					Y					Y		
		الفقرة 5.1.8 عدم توفر الخدمات								Y	Y	Y	Y			Y
		الفقرة 6.1.8 الحظر الذي يفرضه مقدم الخدمة السحابية													Y	
		الفقرة 7.1.8 سوء استعمال الملكية الفكرية		Y	Y				Y		Y					
		الفقرة 8.1.8 فقدان سلامة البرمجيات		Y			Y		Y							

الجدول I.1 – التقابل بين التهديدات والتحديات الأمنية للحوسبة السحابية والقدرات الأمنية

			الفقرة 9 قدرات أمن الحوسبة السحابية												
			الفقرة 1.9 نموذج الثقة	الفقرة 2.9 إدارة خدمات الهوية والنفاذ (IAM)، والاستيقان والترخيص ومراجعة العمليات	الفقرة 3.9 الأمن المادي	الفقرة 4.9 أمن السطوح البينية	الفقرة 5.9 أمن المثيل الافتراضي للحوسبة	الفقرة 6.9 أمن الشبكات	الفقرة 7.9 عزل البيانات وحمايتها وحماية الخصوصية	الفقرة 8.9 التنسيق الأمني	الفقرة 9.9 الأمن التشغيلي	الفقرة 10.9 إدارة الحوادث	الفقرة 11.9 التعافي من الأعطال الكبرى	الفقرة 12.9 تقييم أمن الخدمات ومراجعته	الفقرة 13.9 قابلية التشغيل البيني وقابلية النقل وقابلية الرجوع	الفقرة 14.9 أمن سلسلة التوريد
الفقرة 8 التحديات الأمنية للحوسبة السحابية	الفقرة 2.8 التحديات الأمنية لمقدمة الخدمات السحابية (CSP)	الفقرة 1.2.8 غموض المسؤوليات		Y							Y					
		الفقرة 2.2.8 تقاسم البيئة					Y	Y	Y							
		الفقرة 3.2.8 عدم الاتساق والتضارب في آليات الحماية								Y					Y	
		الفقرة 4.2.8 النزاع القضائي							Y		Y					
		الفقرة 5.2.8 تطور المخاطر									Y				Y	Y
		الفقرة 6.2.8 سوء التحول والتكامل				Y	Y	Y	Y	Y	Y					
		الفقرة 7.2.8 انقطاع الأعمال التجارية										Y	Y			
		الفقرة 8.2.8 الحظر الذي يفرضه الشركاء في الخدمات السحابية														Y
		الفقرة 9.2.8 نقطة ضعف سلسلة التوريد														Y
		الفقرة 10.2.8 الاعتماد على البرمجيات														Y

الجدول I.1 – التقابل بين التهديدات والتحديات الأمنية للحوسبة السحابية والقدرات الأمنية

			الفقرة 9 قدرات أمن الحوسبة السحابية												
			الفقرة 1.9 نموذج الثقة	الفقرة 2.9 إدارة خدمات الهوية والنفاذ (IAM)، والاستيقان والترخيص ومراجعة العمليات	الفقرة 3.9 الأمن المادي	الفقرة 4.9 أمن السطوح البينية	الفقرة 5.9 أمن المثيل الافتراضي للحوسبة	الفقرة 6.9 أمن الشبكات	الفقرة 7.9 عزل البيانات وحمايتها وحماية الخصوصية	الفقرة 8.9 التنسيق الأمني	الفقرة 9.9 الأمن التشغيلي	الفقرة 10.9 إدارة الحوادث	الفقرة 11.9 التعافي من الأعطال الكبرى	الفقرة 12.9 تقييم أمن الخدمات ومراجعته	الفقرة 13.9 قابلية التشغيل البيني وقابلية النقل وقابلية الرجوع	الفقرة 14.9 أمن سلسلة التوريد
الفقرة 8 التحديات الأمنية للحوسبة السحابية	الفقرة 3.8 التحديات الأمنية للشركاء في الخدمة السحابية (CSN)	الفقرة 1.3.8 غموض المسؤوليات		Y							Y						
		الفقرة 2.3.8 سوء استعمال الملكية الفكرية		Y	Y				Y		Y						
		الفقرة 3.3.8 فقدان سلامة البرمجيات		Y			Y		Y								

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

[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 27002] ISO/IEC 27002:2005, *Information technology – Security techniques – Code of practice for information security management*.

[b-ISO/IEC 27005] ISO/IEC 27005:2011, *Information technology – Security techniques – Information security risk management*.

[b-ISO/IEC 28000] ISO/IEC 28000:2007, *Specification for security management systems for the supply chain*.

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

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

[b-NIST-SP-800-53] NIST Special Publication 800-53 Rev.3 (2009), *Recommended Security Controls for Federal Information Systems and Organizations*.

[b-NIST-SP-800-125] NIST Special Publication 800-125 (2011), *Guide to Security for Full Virtualization Technologies*.

[b-NIST-SP-800-145] NIST Special Publication 800-145 (2011), *The NIST Definition of Cloud Computing*.

[b-CSA Matrix] CSA (2013), *Cloud Controls Matrix,* Cloud Security Alliance.

[b-key definition] Key definitions of the Data Protection Act, Information Commissioners Office <http://www.ico.gov.uk/for_organisations/data_protection/the_guide/key_definitions.aspx>

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 (ISDN)
السلسلة J	الشبكات الكبلية وإرسال إشارات تلفزيونية وبرامج صوتية وإشارات أخرى متعددة الوسائط
السلسلة K	الحماية من التداخلات
السلسلة L	بناء الكبلات وغيرها من عناصر المنشآت الخارجية وإنشاؤها وحمايتها
السلسلة M	إدارة الاتصالات، بما في ذلك شبكة إدارة الاتصالات وصيانة الشبكات
السلسلة N	صيانة الدارات الإذاعية الدولية لإرسال البرامج الصوتية والتلفزيونية
السلسلة O	مواصفات أجهزة القياس
السلسلة P	المطاريف وطرائق التقييم الذاتية والموضوعية
السلسلة Q	التبديل والتشوير
السلسلة R	التراسل الإبراقي
السلسلة S	التجهيزات الانتهائية لخدمات الإبراق
السلسلة T	تجهيزات مطرافية للخدمات التلماتية
السلسلة U	التبديل الإبراقي
السلسلة V	اتصالات البيانات على الشبكة الهاتفية
السلسلة X	**شبكات البيانات والاتصالات بين الأنظمة المفتوحة ومسائل الأمن**
السلسلة Y	البنية التحتية العالمية للمعلومات وملامح بروتوكول الإنترنت وشبكات الجيل التالي
السلسلة Z	اللغات والجوانب العامة للبرمجيات في أنظمة الاتصالات

طبعت في سويسرا
جنيف، 2014