الاتحـــــــــــاد الدولـــــــــــي للاتصـــــــــــالات

ITU-T

قطاع تقييس الاتصالات
في الاتحاد الدولي للاتصالات

X.1602
(2016/03)

السلسلة X: شبكات البيانات والاتصالات بين الأنظمة المفتوحة ومسائل الأمن

أمن الحوسبة السحابية – تصميم أمن الحوسبة السحابية

متطلّبات الأمن من أجل بيئات تطبيقات البرمجية كخدمة

التوصية ITU-T X.1602

الاتحاد الدولي للاتصالات

توصيات السلسلة X الصادرة عن قطاع تقييس الاتصالات

شبكات البيانات والاتصالات بين الأنظمة المفتوحة ومسائل الأمن

الشبكات العمومية للبيانات	X.199–X.1
التوصيل البيني للأنظمة المفتوحة	X.299–X.200
التشغيل البيني للشبكات	X.399–X.300
أنظمة معالجة الرسائل	X.499–X.400
الدليل	X.599–X.500
التشغيل البيني لأنظمة التوصيل OSI ومظاهر النظام	X.699–X.600
إدارة التوصيل البيني للأنظمة المفتوحة (OSI)	X.799–X.700
الأمن	X.849–X.800
تطبيقات التوصيل البيني للأنظمة المفتوحة (OSI)	X.899–X.850
المعالجة الموزعة المفتوحة	X.999–X.900
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.1602

متطلّبات الأمن من أجل بيئات تطبيقات البرمجية كخدمة

ملخص

تبحث التوصية ITU-T X.1602 في مستويات اكتمال تطبيقات البرمجية كخدمة (SaaS) وتقترح متطلبات أمن من أجل توفير بيئة متسقة وآمنة لتنفيذ الخدمات لتطبيقات البرمجية كخدمة. وتنطلق المتطلبات المقترحة من موردي الخدمات السحابية (CSP) ومشاركي الخدمات السحابية (CSN) حيث يحتاجون إلى تطبيق من تطبيقات البرمجية كخدمة لتلبية طلباتهم فيما يتعلق بالأمن. وهذه المتطلبات عامة ولا تعتمد على أي خدمة أو نموذج محدد بالسيناريو (مثل خدمات الويب أو نقل الحالة التمثيلية (REST) أو افتراضات أو حلول.

التسلسل التاريخي

الطبعة	التوصية	تاريخ الموافقة	لجنة الدراسات	معرف الهوية الفريد*
1.0	ITU-T X.1602	2016-03-23	17	11.1002/1000/12615

مصطلحات أساسية

متطلبات الأمن، بيئة تطبيقات البرمجية كخدمة (SaaS)، مستوى اكتمال البرمجية كخدمة.

* 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، كان 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.1602

متطلّبات الأمن من أجل بيئات تطبيقات البرمجية كخدمة

1 مجال التطبيق

تركّز هذه التوصية بشكل أساسي على متطلبات أمن بيئات تطبيقات البرمجية كخدمة (SaaS) استناداً إلى مستوى اكتمال هذه التطبيقات. وهذه التوصية موجهة لموردي الخدمات السحابية (CSP) ومشاركي الخدمات السحابية (CSN) مثل مطوّري التطبيقات.

2 المراجع

لا يوجد.

3 التعاريف

1.3 المصطلحات المعرَّفة في وثائق أخرى

تستخدم هذه التوصية المصطلحات التالية المعرَّفة في وثائق أخرى:

1.1.3 خدمة سحابية [b-ITU-T Y.3500]: قدرة أو عدد أكبر من القدرات تُقدم عن طريق الحَوسبة السحابية وتُنفّذ باستخدام سطح بيني محدّد.

2.1.3 فئة الخدمة السحابية [b-ITU-T Y.3500]: طائفة من الخدمات السحابية التي تتّسم بمجموعة مشتركة من الخواص.

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 مورّد خدمة سحابية أو عميل خدمة سحابية أو الاثنين معاً أو يساعد في القيام بهذه الأنشطة.

5.1.3 مورّد الخدمة السحابية [b-ITU-T Y.3500]: طرف يوفر الخدمات السحابية.

6.1.3 مستعمل الخدمة السحابية [b-ITU-T Y.3500]: شخص طبيعي أو كيان يعمل بالنيابة عنه يرتبط بأحد عملاء الخدمة السحابية ويستعمل الخدمات السحابية.

7.1.3 سطح المكتب كخدمة [b-ITU-T Y.3500]: القدرات المقدمة لعميل الخدمة السحابية والتي تمكّنه من القيام عن بُعد بالبناء والتشكيل والإدارة والتخزين والتوصيل لوظائف أسطح مكتب المستعملين.

8.1.3 البنية التحتية كخدمة (IaaS) [b-ITU-T Y.3500]: فئة من الخدمات السحابية تكون فيها القدرات السحابية المقدمة لعميل الخدمة السحابية من نوع قدرات البُنى التحتية.

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

2.3 المصطلحات المعرَّفة في هذه التوصية

لا توجد.

4 الاختصارات والأسماء المختصرة

تستعمل هذه التوصية المختصرات والأسماء المختصرة التالية:

ASP مورد خدمة التطبيق *(Application Service Provider)*

CaaS الاتصالات كخدمة *(Communications as a Service)*

CRM إدارة العلاقة بالعميل *(Customer Relationship Management)*

CSC عميل الخدمة السحابية *(Cloud Service Customer)*

CSN شريك الخدمة السحابية *(Cloud Service Partner)*

CSP مورد الخدمة السحابية *(Cloud Service Provider)*

DaaS سطح المكتب كخدمة *(Desktop as a Service)*

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

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

IdM إدارة الهوية *(Identity Management)*

OLAP المعالجة التحليلية على الخط *(OnLine Analytical Processing)*

OS نظام التشغيل *(Operating System)*

PaaS المنصة كخدمة *(Platform as a Service)*

PKI البنية التحتية للمفتاح العمومي *(Public Key Infrastructure)*

REST نقل الحالة التمثيلية *(Representational State Transfer)*

SaaS البرمجية كخدمة *(Software as a Service)*

SAP نقطة النفاذ إلى الخدمة *(Service Access Point)*

SLA اتفاق مستوى الخدمة *(Service Level Agreement)*

5 الاصطلاحات

لا توجد.

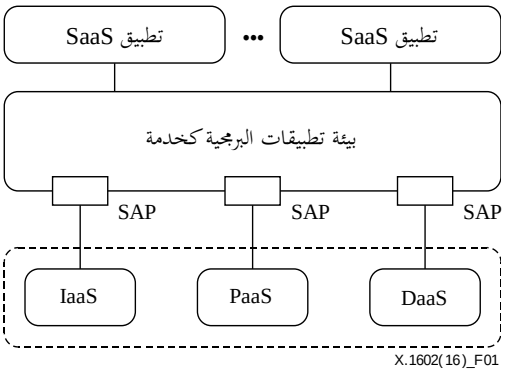
6 نظرة عامة

بيئة تطبيقات البرمجية كخدمة (SaaS) هي بيئة للتطوير والنشر والتنفيذ متعددة الشاغلين متمحورة حول الخدمة، تتم فيها استضافة البرمجية وما يرتبط بها من بيانات مركزياً ويتم النفاذ إليها عادةً من المستعملين حسب الطلب باستخدام عميل، مثل متصفّح ويب، عبر الإنترنت.

وعلى الرغم من أن هذه التوصية تتعلق في الأساس بالبرمجية كخدمة، فإن بعض المفاهيم الواردة فيها يمكن أن تطبّق أيضاً على فئات أخرى للخدمات السحابية تتضمن أيضاً نوع قدرات التطبيقات، مثل الاتصالات كخدمة (CaaS).

ويصوّر الشكل 1 نموذجاً مفاهيمياً لبيئة تطبيقات البرمجية كخدمة. وسيتم دمج القدرات الأساسية من البنية التحتية كخدمة (IaaS) والمنصة كخدمة (PaaS) وسطح المكتب كخدمة (DaaS) وتغليفها في شكل خدمات مع توفير نفاذ مؤمّن باستعمال نقطة نفاذ إلى الخدمة (SAP) مصدرة. وفي هذه التوصية توفر سحابات البنية التحتية كخدمة خدمات الحوسبة وخدمات التخزين وخدمات الشبكة؛ فيما توفر سحابات المنصة كخدمة خدمة المنصة وتوفر سحابات سطح المكتب كخدمة خدمة سطح المكتب لبيئة من بيئات تطبيقات البرمجية كخدمة. وتشكل كل هذه الخدمات لَبِنات البناء الأساسية لتطوير تطبيق.

كما توفر البيئة بعض وظائف إدارة الخدمة الضرورية بما في ذلك تسجيل الخدمة وتشكيلها وتناغمها والتحكم في النفاذ إليها وعزلها ومراقبتها وغير ذلك من وظائف التحكم في الخدمة.



الشكل 1 – نموذج مفاهيمي لبيئة تطبيقات البرمجية كخدمة

7 مستويات اكتمال تطبيقات البرمجية كخدمة

يصنف اكتمال تطبيقات البرمجية كخدمة في الصناعة إلى أربعة مستويات يمكن تسميتها بمستوى العميل والمستوى القابل للتشكيل ومستوى الشاغلين المتعددين ومستوى مدى إمكانية التوسّع. ويغطي كل مستوى خصائص المستوى الذي يسبقه ويوفر خصائص موسّعة. ويعرض الجدول 1 المخطط الذي يمثل خصائص نماذج الاكتمال المختلفة لتطبيقات البرمجية كخدمة.

الجدول 1 – مخطط لمستوى اكتمال تطبيقات البرمجية كخدمة

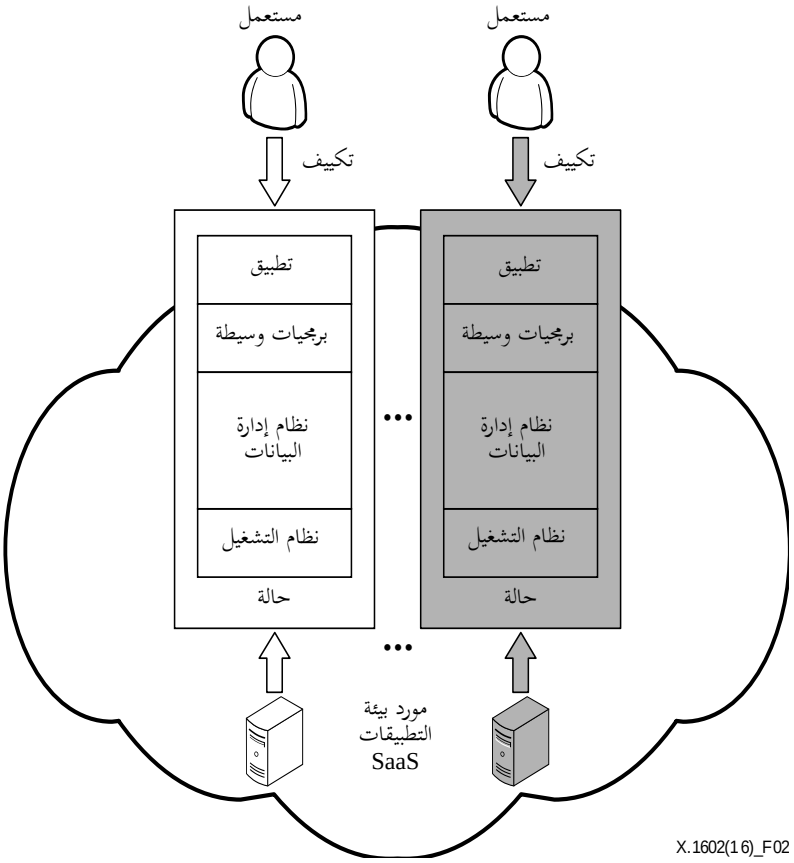
	العميل	قابل للتشكيل	شاغلون متعددون	قابل للتوسع
المستويات	الشاغل 1 الشاغل 2 الشاغل 3 الحالة 1 الحالة 2 الحالة 3	الشاغل 1 الشاغل 2 الشاغل 3 الحالة الحالة الحالة	الشاغل 1 الشاغل 2 الشاغل 3 الحالة	الشاغل 1 الشاغل 2 الشاغل 3 وحدة تحقيق التوازن في حمل الشاغلين الحالة الحالة الحالة

X.1602(16)_Table01

ولمستويات الاكتمال المختلفة لتطبيقات البرمجية كخدمة متطلبات أمن مختلفة لبيئات تطبيقات البرمجية كخدمة وستوضح هذه المتطلبات من منظور موردي الخدمات السحابية ومشاركي الخدمات السحابية في الفقرة 8.

1.7 المستوى 1: تطبيق SaaS للعميل

تطبيق SaaS للعميل هو نموذج مماثل لتوصيل مورد خدمة تطبيق (ASP) تقليدي لبرمجية. ولكل عميل الحل الملائم له للتطبيق SaaS ويقوم بتشغيل حالة التطبيق الفردية الخاصة به على مخدّم سحابي. وكما هو موضح في الشكل 2، تتألف حالة تطبيق العميل من بيئة التنفيذ بالكامل بما في ذلك نظام التشغيل (OS) ونظام إدارة البيانات والبرمجيات الوسيطة الخاصة بكل واحد من الشاغلين وعلى مورّد بيئة البرمجية كخدمة (SaaS) رعاية الحالات المتعددة. وهذا النموذج صعب التوسع للوفاء بطلبات الاحتياجات المتزايدة للعملاء، ويمكن أن يكون تشغيله مُكلفاً.

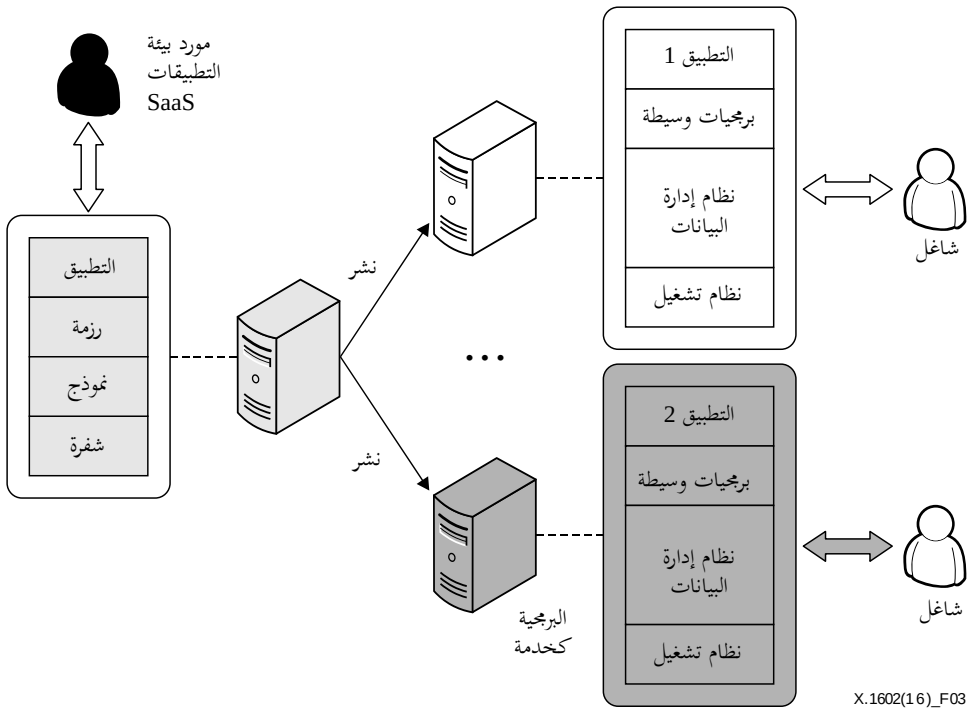


الشكل 2 – معمارية التطبيق SaaS للعميل

ويمكن بسهولة تحويل تطبيقات نموذج مخدّم العميل النمطية إلى تطبيقات SaaS للعميل بنقل المخدّمات إلى السحابات مع تعديل طفيف نسبياً. والتطبيقات المناسبة لهذا السيناريو تطوّر عادةً بمتطلبات خاصة من الشركة أو المنظمة. ويُولى اعتبار كبير للأمن في النظام نفسه، ومن ثم، فإن الأسلوب الاعتيادي يتمثل في تجميع مجموعة من الآلات المادية في منطقة خصوصية ونشر نظام لإدارة البيانات (يوفر طرائق مجردة من استمرارية مختلف أنواع البيانات وعملياتها) والبرمجية المصاحبة عليها. والنظام مصمّم فقط للاستعمال الداخلي مع وسائل صارمة للتحكم في النفاذ. ونموذج حالة التطبيق واحد لجميع العملاء ويوفر قدرة تشكيل محدودة. ومع ذلك فإن الحالة بالنسبة لكل عميل مستقلة تماماً عن الحالات الأخرى.

2.7 المستوى 2: التطبيق SaaS القابل للتشكيل

بالنسبة لبعض التطبيقات الشائع استعمالها وغير المكيّفة حسب العميل، مثل نظام بناء موقع ويب ذاتي الخدمة، يوفر موردو التطبيقات SaaS نماذج مشتركة لهذه التطبيقات ومجموعات عديدة من بيئات وقت التشغيل من أجل حالات هذه التطبيقات. واستناداً إلى وجود نموذج واحد، يمكن للعملاء استحداث حالات منفصلة ومتعددة من التطبيق عن طريق تشكيل المنظر الذي يظهر عليه التطبيق وسلوكه، حيث يتم نشره وتنفيذه على آلات الأفراد الافتراضية أو المادية لتلبية احتياجاتهم المكيّفة. وحالات التطبيق معزولة عن بعضها. وتُعرض المعمارية في الشكل 3.



الشكل 3 – معمارية تطبيق SaaS قابل للتشكيل

ويتسم التطبيق SaaS القابل للتشكيل بالخصائص التالية:

1) التطبيق في النشر الأولي يكون نسخة من مُنتج قياسي يقوم الشاغلون بتشكيله لكي يلائم احتياجاتهم الخاصة. بيد أن خيارات تشكيل المنتج محدودة.

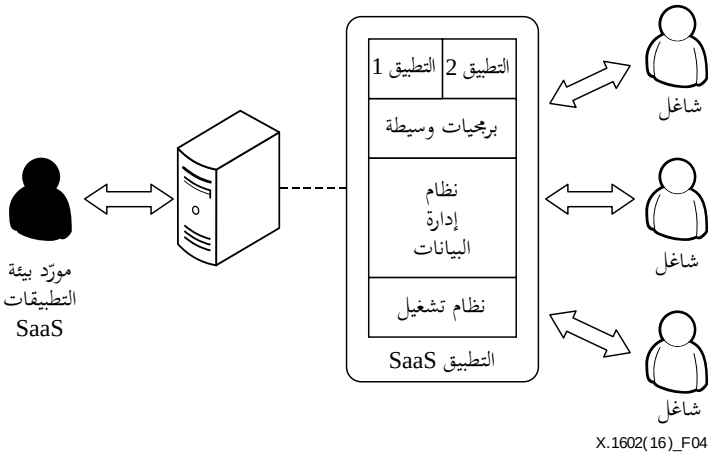
2) بالنسبة لمورّدي التطبيقات SaaS، يمكن بسهولة تطبيق أيّ تعديلات على شفرات المنتج بالنسبة لجميع الشاغلين في الحال. ومع ذلك لا يناسب كل حالة إلاّ تحديث أو استمثال طفيف لشفرات المنتج، وذلك بسبب مشكلة التوافق الأمامي التي قد تنتج عن التحديث أو الاستمثال.

3) يقوم الشاغلون بتخزين البيانات في آلاتهم الافتراضية أو المادية المعزولة عن بعضها. ونتيجة لذلك، يتعيّن على مورّد بيئة التطبيقات SaaS أن يوفر موارد كافية كسعات التخزين لدعم العدد الكبير المحتمل لحالات التطبيق التي تعمل في وقت واحد.

ومع تطوّر وتحسّن تكنولوجيا البرمجيات، سيتم توفير التطبيق مع خيارات تشكيل كافية لتلبية المتطلبات المكيّفة للمستعملين ولكي تكون عملية التشكيل والاستعمال أكثر ذكاءً وأتمتةً. وسيقوم موردو التطبيقات SaaS بتقسيم المنتجات إلى إصدارات مختلفة لكي تتطابق مع المستويات المختلفة للشاغلين.

3.7 المستوى 3: التطبيق SaaS متعدد الشاغلين

في هذا المستوى، يمكن لمورّد التطبيقات SaaS، بمساعدة البيانات الشرحية القابلة للتشكيل، أن يوفر حالة وحيدة تخدم شاغلين متعددين في وقت واحد. ويمكن تفعيل تعدّد الشاغلين في طبقات مختلفة بما في ذلك نظام التشغيل ونظام إدارة البيانات والبرمجيات الوسيطة والتطبيق. ويدخل معرّف هوية للشاغل من أجل التمييز بين العملاء المختلفين. وعند استعمال قاعدة بيانات في نظام لإدارة البيانات، يوسع مخطط قاعدة البيانات بحيث يضمّ معلمة هوية الشاغل لتخزين بيانات جميع العملاء في مجموعة الجداول نفسها. وهوية الشاغل لازمة أيضاً في استفسارات قاعدة البيانات من أجل استرجاع البيانات لعميل بعينه. ويوضح الشكل 4 المعمارية العامة للتطبيق SaaS متعدد الشاغلين.



الشكل 4 – معمارية التطبيق SaaS متعدد الشاغلين

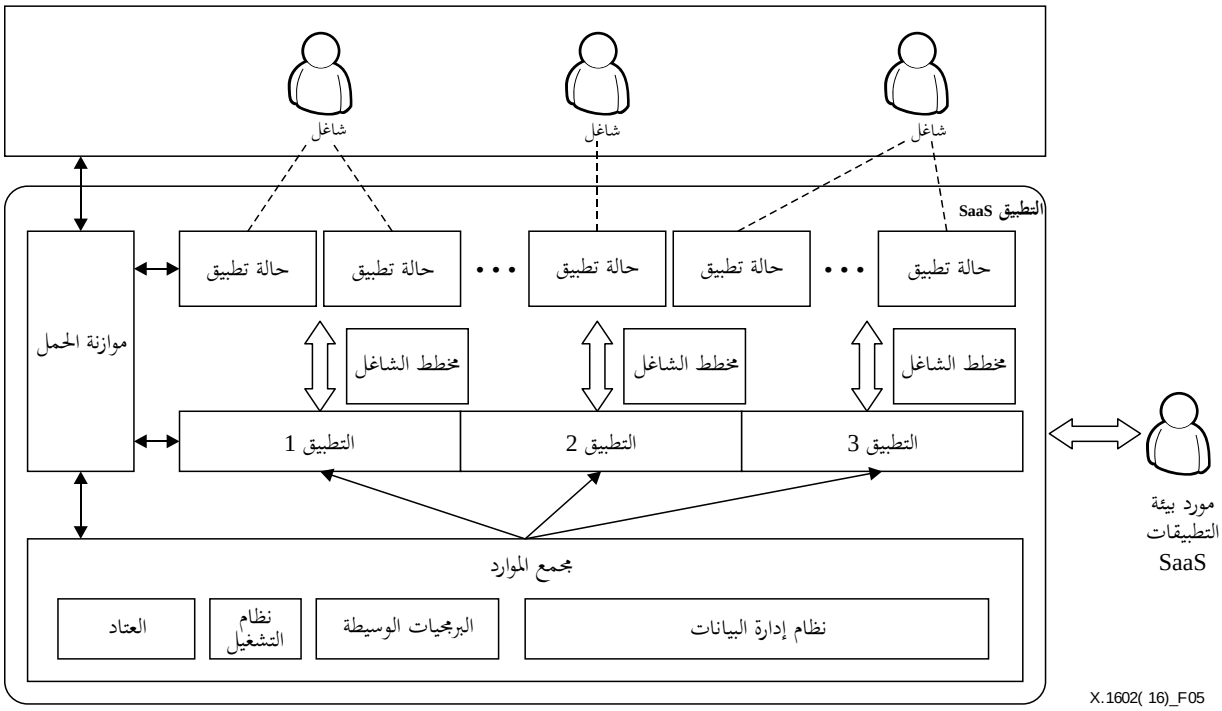
التطبيق SaaS الذكي الخاص بشركات الأعمال، كإدارة العلاقات مع العملاء (CRM)، يُعد تنفيذاً مثالياً لهذا المستوى. وحتى الآن، تمّ بذل المزيد من الجهود للجمع بين تخزين البيانات والحَوسبة السحابية من جهة والتطبيقات SaaS من جهة من أجل توفير تطبيقات ذكية على الخط لشركات الأعمال. وتتمّ استضافة مستودع البيانات في مركز البيانات ويتم التحديد المسبق للتطبيقات الذكية ونماذج البيانات الخاصة بشركات الأعمال بحيث يتم استعمالها بالقدر الزهيد من التكييف. وبالنسبة للشاغلين، فكل ما عليهم القيام به هو انتقاء عناصر البيانات اللازمة للتطبيقات الذكية لشركات الأعمال وتحديد تقابل البيانات بين مصادر البيانات ومستودع البيانات ونماذج البيانات. ويقوم النظام بدمج البيانات الخاصة بأنظمة مصادر متعددة في مستودع البيانات لدعم تطبيقات المعالجة التحليلية على الخط (OLAP) باستعمال نصوص مُعدّة أوتوماتياً. وخلال وقت التشغيل، فإن الحالة الواحدة من التطبيقات الذكية لشركات الأعمال تخدم في العادة العديد من الشاغلين في نفس الوقت باستعمال تقنيات البيانات الشرحية. وتضمن التخويلات والسياسات الأمنية أن النفاذ إلى بيانات وتطبيقات كل عميل معزول عن النفاذ إلى بيانات وتطبيقات العملاء الآخرين.

ويوفر هذا المستوى قدراً أكبر بكثير من الكفاءة من استعمال موارد الحوسبة والتخزين وبالتالي يمكن أن يؤمّن خدمة عدد أكبر من الشاغلين. ويمكن أيضاً تحقيق أداء مقارن مع إمكانية التوسّع والمرونة بمساعدة تقسيم البيانات وتقنيات موازية.

وإمكانية التشكيل وكفاءة الشاغلين المتعددين هما الخاصيّتان المميّزتان لهذا المستوى من التطبيقات SaaS.

4.7 المستوى 4: التطبيقات SaaS القابلة للتوسّع

يخدم معظم مورّدي خدمات الويب عدداً كبيراً بشكل اعتباطي من العملاء كشاغلين متعددين. وبالتالي، فإن كل طبقة من معمارية المنصّة الأساسية من العتاد إلى التطبيق، يتعيّن أن تكون قابلة للتوسع بسهولة فيما يتعلق بالتطبيقات والخدمات كما هو موضّح في الشكل 5. ومن ثم يمكن إضافة المزيد من الشاغلين والمزيد من المستعملين لكل شاغل دون الحاجة إلى أيّ أعمال إضافية فيما يتعلق بإعادة تصميم معمارية التطبيقات.



الشكل 5 – معمارية التطبيق SaaS القابل للتوسّع

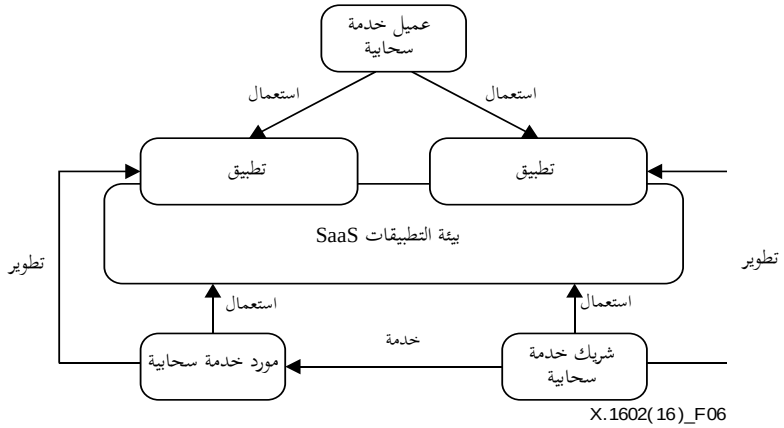
بالنسبة لطبقة التطبيق، عندما يكون هناك شاغل جديد، ستتولد حالة تطبيق واحدة أو أكثر حسب الاحتياجات الخاصة بالشاغل أو يتم اختيار حالة مناسبة قائمة طبقاً لاحتياجات تقوم على آلية موازنة الحمل. وجميع حالات التطبيق في بيئة كهذه يتعيّن أن تتولّد دينامياً.

والموارد الأساسية للتطبيقات SaaS القابلة للتوسّع تدعم أيضاً التوسّع المرن. فأيّ جزء من العتاد أو البرمجيات الوسيطة أو البرمجيات أو البيانات سيتعيّن إدارته في مجمع الموارد. وتحصل التطبيقات على كل ما تحتاج إليه من موارد من مجمع الموارد دينامياً. ويجوز إضافة موارد جديدة دون إعادة التجميع أو إعادة تصميم المعمارية إذا استدعى الأمر.

وهناك اعتبارات متعدّدة للتصميم فيما يتعلق بتكنولوجيات التوسّع الدينامية بما في ذلك اختيارات التوسّع وتوزيع الموارد واتفاق مستوى الخدمة (SLA) وما إلى ذلك. ويمكن تنفيذ أي شاغل جديد بوصفه حالة وحيدة أو يمكن أن يتعايش مع شاغلين آخرين على حالة مشتركة. والحالات المختلفة التي تدير أنواعاً مختلفة من الشاغلين يمكن توزيعها لموارد متغيّرة. وينبغي لمورّد بيئة التطبيقات SaaS أن ينظر في اتفاقات مختلفة لمستوى الخدمة لمختلف الشاغلين عند استخدام موازنة الحمل والموارد المشتركة.

8 متطلّبات الأمن لبيئة التطبيقات SaaS

يعرض الشكل 6 العلاقة بين عميل الخدمة السحابية (CSC) ومورد الخدمة السحابية (CSP) وشريك الخدمة السحابية (CSN) فيما يتعلق ببيئة التطبيقات SaaS التي يكون فيها لكل من مورّد الخدمة السحابية وشريك الخدمة السحابية أدوار مختلفة للقيام بالوظائف المختلفة. ويمكن لشريك الخدمة السحابية أن يخدم مورّد الخدمة السحابية كمورّد محتوى أو مورّد برمجية أو مكامل للنظام أو مراجع، في حين يمكن لكل من شريك الخدمة السحابية ومورد الخدمة السحابية تطوير تطبيقات لعميل الخدمة السحابية. ولمورد الخدمة السحابية وشريك الخدمة السحابية سطوح بينية مع بيئة التطبيقات SaaS، في حين يتفاعل عميل الخدمة السحابية فقط مع التطبيقات الخاصة به. ونتيجةً لذلك، تركّز هذه التوصية في الأساس على متطلّبات الأمن لبيئة التطبيقات SaaS بالنسبة لمورد وشريك الخدمة السحابية في نموذج اكتمال مختلف. وتتحدد متطلّبات الأمن لبيئة التطبيقات SaaS من جانب مورّد وشريك الخدمة السحابية وهما يشترطان أن تكون لهذه البيئة القدرة على الوفاء بمتطلّباتهما فيما يتعلق بالأمن.



الشكل 6 – العلاقة بين عميل ومورّد وشريك الخدمة السحابية

لمورّد وشريك الخدمة السحابية متطلّبات الأمن الخاصة بهما فيما يتعلق بالبيئة في مستويات مختلفة من التطبيقات SaaS. ويوضح الجدول 2 متطلّبات الأمن لمورّد وشريك الخدمة السحابية في بيئة التطبيقات SaaS. والمتطلّبات التي يمكن تطبيقها على كل من مورّد وشريك الخدمة السحابية تعتبر متطلّبات مشتركة.

الجدول 2 – متطلّبات الأمن لمورد وشريك الخدمة السحابية في بيئة التطبيقات SaaS

	بيئة التطبيقات SaaS
متطلّبات مشتركة	إدارة الهوية والنفاذ وأمن البيانات وتقييم الأمن ومراجعته وأمن السطح البيني وتقوية الأمن.
مورد الخدمة السحابية	التيسُّر وضمان قابلية التشغيل البيني/تنقلية الخدمة وحماية أصول البرمجيات والالتزام القانوني والتحقق الأمني من شفرات المصدر.
شريك الخدمة السحابية	أمن المراجعة وأمن البرمجيات وإمكانية صيانة البرمجيات.

1.8 متطلّبات الأمن المشتركة

لكلّ من مورد وشريك الخدمة السحابية العديد من متطلّبات الأمن المشتركة في بيئة التطبيقات SaaS.

1.1.8 إدارة الهوية والنفاذ (IAM)

1.1.1.8 إدارة الهوية (IdM)

يشترك في بيئة التطبيقات SaaS العديد من المديرين والمستعملين، حيث يمكن النفاذ إليها واستعمالها داخلياً (CSP) وخارجياً (CSN). وتدعو الحاجة إلى إدارة الهوية (IdM) ليس فقط من أجل حماية الهويات بل لتسهيل عمليات إدارة النفاذ والاستيقان والتخويل ومراجعة المعاملات في بيئة التطبيقات SaaS هذه الدينامية والمفتوحة.

وبالنسبة لجميع نماذج الاكتمال، ينبغي لإدارة الهوية أن تمكّن من تنفيذ تسجيل دخول وحيد و/أو اتحاد للهويات من أجل بيئة التطبيقات SaaS باستعمال آليات استيقان متغيّرة في ميادين أمنية مختلفة.

2.1.1.8 نموذج الثقة

يتعيّن أن تضم بيئة التطبيقات SaaS نموذج ثقة شامل لكل من مستوى الشاغلين المتعددين والمستوى القابل للتوسّع. ومن شأن نموذج الثقة هذا أن يمكّن من إقامة جزر و/أو اتحادات من الكيانات الموثوقة. وبالتالي سيكون بإمكان نظام إدارة بيئة التطبيقات SaaS والموارد الأساسية والمشرفين الفائقين والآليات والتطبيقات الافتراضية التي تقوم على بيئة التطبيقات SaaS استيقان الهويات والحقوق المخوّلة لكيانات ومكوّنات أخرى. ويستند كل من جزر أو اتحادات الثقة إلى واحدة أو أكثر من السلطات الموثوقة (مثلاً سلطة إصدار شهادات البنية التحتية للمفاتيح العمومية (PKI)).

3.1.1.8 إدارة النفاذ

يتعيّن على مديري بيئات التطبيقات SaaS أن يوفروا آليات تفوض التخويل لمديري الشاغلين. ويمنح مديرو الشاغلين حقوق النفاذ لمواردهم المقابلة. وينبغي لإدارة النفاذ لبيئة تطبيقات SaaS كهذه أن تدعم نماذج متعددة للتحكم في النفاذ مثل النموذج القائم على الهوية والنموذج القائم على الاستراتيجية والنموذج القائم على الدور والنموذج القائم على المهمة وغيرها.

وبالنسبة للتطبيقات SaaS من مستوى العميل والمستوى القابل للتشكيل، يعتبر نموذج التحكم في النفاذ القائم على الدور شرطاً أساسياً. فعلى سبيل المثال، فإن شريك الخدمة السحابية الذي يدعم بناء الخدمة من مورّد الخدمة السحابية، قد يكون مسؤولاً عن بعض التطبيقات ولكنه لا يتمتع بحقوق إدارة نظام الخدمة السحابية بأكمله. وإلى جانب ذلك، قد يسمح لشريك الخدمة السحابية بالنفاذ فقط إلى جزء من الموارد بحقوق نفاذ ممنوحة. ومع ذلك، يمكن لشريك الخدمة السحابية أن يتقاسم موارده بتوفير سطوح بينية للتطبيقات لشركاء آخرين في الخدمة السحابية.

وبالنسبة لمستوى الشاغلين المتعددين والمستوى القابل للتوسع، يتعيّن دمج نموذج تحكّم في النفاذ لكل فرد ولكل مجموعة. وبالنسبة للتحكم في النفاذ القائم على الدور، ينبغي استخدام تقاسم الموارد بين الشاغلين المتعددين طبقاً لمجموعات المهام في أيّ تدفق للأعمال والحقوق الممنوحة لهذه المهام. ولذا، فإنه ينبغي لبيئة التطبيقات SaaS عند تنفيذ مجموعات المهام هذه أن تحدد آلية دعم التحكم في النفاذ القائم على المهمة. وتستخدم هذه الآلية للتأكد من حقوق نفاذ الشاغلين للموارد الأساسية يمكن أن تمنح وتسحب في الوقت المناسب ومنع الاستعمال غير المخول للموارد الأساسية.

2.1.8 أمن السطح البيني

يتعيّن أن تؤمن بيئة التطبيقات SaaS السطوح البينية المفتوحة على مورّدي أو شركاء الخدمة السحابية التي توصل أو تطور من خلالها الأنواع المختلفة لخدمات الحوسبة السحابية، كما يتعيّن أن تؤمن الاتصالات استناداً إلى هذه السطوح البينية. والآليات المتاحة لضمان أمن السطح البيني تشمل على سبيل الذكر وليس الحصر: الاستيقان من طرف واحد/المتبادل والتحقق من السلامة والتوقيع الرقمي وما إلى ذلك.

3.1.8 أمن البيانات

1.3.1.8 فرز البيانات

يمكن فرز البيانات مادياً أو منطقياً. والفرز المادي للبيانات ينبغي أن يكون مصحوباً بالتحكم في النفاذ إلى المخازن المادية. وينبغي لبيئة التطبيقات SaaS أن تلتزم بتخزين بيانات مختلف الشاغلين في مناطق مختلفة من المخزن المادي أو تطبيق التحكم في النفاذ إلى البيانات لمختلف الشاغلين من خلال تصاريح النفاذ أو ميادين البيانات أو أيّ طريقة أخرى. ويستوجب الفرز المنطقي للبيانات أن يمنع مختلف الشاغلين من النفاذ إلى بيانات الآخرين باستخدام تقنيات مثل إضفاء الطابع الافتراضي، حتى وإن كانت جميع البيانات مخزّنة معاً.

وبالنسبة للتطبيقات SaaS من مستوى العميل والمستوى القابل للتشكيل، تخزن بيانات كل شاغل بشكل منفصل وتُعزل عن الآخرين على المستوى المادي.

وبالنسبة للتطبيقات SaaS من مستوى الشاغلين المتعددين والمستوى القابل للتوسع، تخزن بيانات جميع الشاغلين في السحابات. وبالتالي، يلزم أن تكون بيئة التطبيقات SaaS ذكية بما يكفي لفصل البيانات من الشاغلين المختلفين والحفاظ على العزل فيما بين بيانات الشاغلين المختلفين سواء عند المعالجة أو الإرسال. وينبغي ضمان الحدود بين كل شاغل على المستوى المادي أو على المستوى المنطقي، وهو ما يتوقف على التفتّت المطلوب للعزل والنشر المحدد لبرمجيات وعتاد الحوسبة السحابية.

2.3.1.8 سرية البيانات

في معظم الحالات، تقوم بيانات الشاغل على التخزين والاستخدام خارج المنشأة وتخضع للكشف. وبالتالي، يلزم أن تدعم بيئة التطبيقات SaaS آليات تجفير لضمان سرية البيانات عند الإرسال أو خلال المعالجة أو خارج العمل ومنع تسرّب البيانات بسبب مواطن ضعف في التطبيق.

وخدمة تجفير البيانات ضرورية لجميع مستويات التطبيقات SaaS. ويتعيّن تجفير البيانات الحساسة لمنع كشفها.

وبالنسبة لمستوى الشاغلين المتعددين والمستوى القابل للتوسع، حيث إنه يتعيّن تخزين بيانات الشاغلين في قاعدة بيانات واحدة أو حتى في جدول واحد كبير، فإنه يلزم أن توفر بيئة التطبيقات SaaS آلية مناسبة لإدارة المفاتيح من أجل ضمان عدم إمكانية سطو شاغلين آخرين للبيانات.

3.3.1.8 سلامة البيانات

البيانات بما في ذلك بيانات النظام وبيانات المستعمل، مثل السجلات وبيانات التشكيل، تستوجب أن تدعم بيئة التطبيقات SaaS آليات السلامة لمنع التلاعب فيها من جانب غير المخوّلين عند إرسالها أو أثناء معالجتها أو خارج العمل.

ويتعيّن عدم تعديل سجل النظام وسجل التطبيق. وفي هذه الحالة، عند وقوع أعطال أو الاستعمال الخطأ، يمنع مورد الخدمة السحابية والبرمجيات الضارة من إخفاء الأثر عن طريق تعديل السجلات.

وقد يتعيّن أن يُتاح لعملاء الخدمة السحابية تشكيل التطبيق SaaS عند الطلب. وبيانات التشكيل مثل ملف التشكيل يتعيّن عدم تعديلها هي الأخرى بدون تخويل.

وفي بيئة التطبيقات SaaS، تخزّن بيانات المستعملين في سحابات يديرها مورّد الخدمة السحابية. وفي هذه الحالة، يصبح التحقق من سلامة البيانات من متطلبات الأمن الهامة. وعلاوةً على ذلك، يتعيّن التحقق من سلامة البيانات هائلة الحجم.

4.3.1.8 موثوقية البيانات

لدعم موثوقية البيانات، يلزم أن تدعم بيئة التطبيقات SaaS آليات إعداد نسخ احتياطية للبيانات أو آليات الإطناب لضمان إمكانية نفاذ الشاغلين إلى البيانات حتى إذا فقد جزء من عقد التخزين السحابية كفاءته.

ويتعيّن أن تقوم البيانات المستضافة بإعداد احتياطي لمواقع متعددة؛ وإلاّ، فإن البيانات ستكون غير فعالة بشكل كامل. ويلزم أن يكون لبيئة التطبيقات SaaS القدرة على الاستعادة الكاملة للبيانات وتخزينها في الوقت المحدد إضافة إلى الحفاظ على تزامن البيانات من أجل ضمان اتساق النسخ المتعددة.

5.3.1.8 تتبُّع البيانات والتحكّم فيها

يلزم أن تضمن بيئة التطبيقات SaaS أن الموقع المادي للبيانات يمتثل للقوانين واللوائح المحلية السارية ولأي قيود مُدرجة في الاتفاقات القانونية. ويتعيّن أن توفر بيئة التطبيقات SaaS طرائق تمكّن عملاء الخدمة السحابية من تحديد مواقع تخزين بياناتهم والتحقق من وجود بياناتهم في المكان المناسب.

ومن الشواغل الرئيسية في البُنى التحتية المتقاسمة والافتراضية ليس فقط فقدان سيطرة المستعملين على بياناتهم، ولكن أيضاً وضع البيانات في مواقعها والتحكم في دورة حياتها بالكامل. وفي أي وقت محدد، يتعيّن أن تعرف بيئة التطبيقات SaaS بدقة مكان تخزين ومعالجة كل بيانات النظام وبيانات المستعمل وتتيح لعملاء الخدمة السحابية إمكانية التحقق من موقع البيانات. ويجب ألاّ يسمح، سواء أثناء الاستعمال أو بعده، لأطراف ثالثة غير مخوّلة (بما في ذلك موردو الخدمة السحابية) من تتبّع حركة البيانات.

4.1.8 تقييم الأمن ومراجعته

عندما يطرأ على الموارد الأساسية تغيير أو تتعرّض للسطو أو تعمل بشكل غير سليم، يتعيّن أن تكون بيئة التطبيقات SaaS قادرة على استهلال إجراء تقييم أمني من أجل تحديد ما إذا كانت الخدمات الأمنية المحددة أو سياساتها الأمنية المطبّقة قد تأثرت أم لا، وما إذا كان يُقترح الإعلان عن مؤشرات أو إرشادات إذا تعذَّر عليها الوفاء بشروط محددة سلفاً. وينبغي تفويض طرف مخوّل سلطة التحقق من أن بيئة التطبيقات SaaS تمتثل لمتطلّبات الأمن المطبقة. ويمكن إجراء التقييم الأمني أو المراجعة الأمنية بواسطة عميل الخدمة السحابية (CSC) أو مورد الخدمة السحابية (CSP) أو طرف ثالث (شريك الخدمة السحابية (CSN))، كما يمكن اعتماد شهادات أمنية بواسطة طرف ثالث مخوّل (CSN).

وينبغي استخدام أطراف ثالثة موثوقة مستقلة لتوفير تقييمات أو مراجعة أمنية موثوقة ومستقلة وحيادية.

5.1.8 تقوية الأمن

تهدف بيئة التطبيقات SaaS في الأساس إلى توفير خدمة مؤمّنة متمحورة حول بيئة تطوير ونشر وتنفيذ متعددة الشاغلين للتطبيقات SaaS. وتكون الخواص الأمنية للتطبيقات SaaS غير كافية أو غير مُعدّة بشكل جيد في بعض الأحوال. ويتعيّن أن تقوم بيئة التطبيقات SaaS باسترجاع الخواص الأمنية الضعيفة هذه للتطبيقات SaaS والتحقق منها وتوفير آليات تفاضلية لتقوية الأمن من أجل تعزيز التطبيقات SaaS طبقاً لهذه الخواص الأمنية الضعيفة من أجل الوفاء بمتطلّبات الأمن لمختلف الشاغلين في السياقات المختلفة. وتتألف الخواص الأمنية للتطبيقات من خواص أمنية سكونية عندما تكون التطبيقات في حالة خمول ومن خواص أمنية ديناميكية عندما تكون التطبيقات قيد التشغيل.

2.8 متطلّبات الأمن لمورد الخدمة السحابية

إضافة إلى متطلّبات الأمن المشتركة، لمورّد الخدمة السحابية متطلّبات أمن محدّدة في بيئة التطبيقات SaaS.

1.2.8 التيسُّر

بالنسبة لمورّد الخدمة السحابية، يتعيّن أن تضمن بيئة التطبيقات SaaS أن عملاء الخدمة السحابية مخدومون طوال الوقت وهو ما يستلزم معالجة أعطال العتاد/البرمجيات وهجمات رفض الخدمة وما إلى ذلك. ومن الضروري ضمان الحدّ الأدنى من زمن الانقطاع لعملاء الخدمة السحابية.

2.2.8 ضمان قابلية التشغيل البيني/التنقلية للخدمة

عندما يرغب عميل الخدمة السحابية في نقل نظامه بالكامل أو جزء منه لمورّد آخر للخدمة السحابية، يلزم مورد الخدمة السحابية الأصلي بيئة التطبيقات SaaS بتوفير ضمان لقابلية التشغيل البيني/التنقلية للخدمة من أجل تدنية الأضرار التي تلحق بأعمال عميل الخدمة السحابية. وإلى جانب ذلك، يجب أن تضمن بيئة التطبيقات SaaS أن البيانات ذات الصلة ستُحذف تماماً من مورد الخدمة السحابية السابق ولن يتسنّى استردادها بواسطة أي أطراف أخرى.

3.2.8 حماية أصول البرمجيات

في بيئة التطبيقات SaaS، تتعين حماية أصول البرمجيات (مثل التطبيقات والبيانات الداخلية للتطبيقات والنصوص ومجموعات الإرشادات ومكتبة شفرات الوظائف وترخيص البرمجية وما إلى ذلك).

ويلزم مورد الخدمة السحابية بيئة التطبيقات SaaS بحماية السرية والسلامة إذا ما قام مورد أو شريك الخدمة السحابية بتوفير أصول برمجيات، وهو ما يستلزم عدم إمكانية نسخ هذه الأصول أو إساءة استعمالها أو التلاعب بها أو منحها بالمجان أو استعمالها بشكل غير مخوّل.

4.2.8 الامتثال القانوني

على الرغم من أنه بإمكان مورّد الخدمة السحابية استعمال آليات إعداد نسخ احتياطية أو آليات الإطناب للبيانات من أجل ضمان موثوقية بيانات عملاء الخدمة السحابية، فإنه يتعيّن أن تضمن بيئة التطبيقات SaaS أن نسخ البيانات لن تبقى لمدة أطول من المدة المسموح بها طبقاً لقانون حماية البيانات المعمول به.

5.2.8 التحقّق الأمني من شفرات المصدر

كما هو الحال بالنسبة لبيئة التطبيقات SaaS، يجوز لشريك الخدمة السحابية أن يوفر شفرات للتطبيقات أو محتوى أو برمجيات لمورد الخدمة السحابية، وهنا يلزم أن توفر بيئة التطبيقات SaaS آليات تساعد مورد الخدمة السحابية على التحقق من الشفرات وتفادي الشفرات الضارة.

3.8 متطلّبات الأمن لشريك الخدمة السحابية

في بيئة التطبيقات SaaS، قد يكون شريك الخدمة السحابية مطوّراً للتطبيقات ومورداً للمحتوى ومورداً للبرمجيات ومكاملاً للنظام ومراجعاً. فإلى جانب متطلّبات الأمن المشتركة، لشريك الخدمة السحابية متطلبات أمن خاصة به في بيئة التطبيقات SaaS.

1.3.8 أمن المراجعة

عندما يكون شريك الخدمة السحابية مراجعاً، يتعيّن أن توفر بيئة التطبيقات SaaS آليات تساعد شريك الخدمة السحابية على جمع أحداث المراجعة والتسجيل والإبلاغ عن المعلومات على مستوى تفتّت الشاغل والتطبيق. وتستعمل المعلومات من أجل ضمان امتثال خدمة مورد الخدمة السحابية للمتطلّبات التنظيمية الحكومية والاتفاقات القانونية المبرمة مع الشاغلين. كما يجب أن توفر بيئة التطبيقات SaaS آليات تساعد شريك الخدمة السحابية على التأكد من أن المعلومات التي تجمع وتبلّغ بواسطة مكونات المراجعة داخل نظام مورّد الخدمة السحابية صحيحة وغير عرضة للتلاعب أو الاحتيال.

وبالإضافة إلى ذلك، يجب أن تزوّد بيئة التطبيقات SaaS شريك الخدمة السحابية بإمكانية تسجيل التغييرات في البيانات الهامة ومراقبة تيسّر البيانات على الخط من أجل إرسال إنذار أمني في الوقت المحدد ومن ثم تقليل الخسائر.

2.3.8 أمن البرمجيات

عندما يكون شريك الخدمة السحابية مطوّر محتويات أو برمجيات سحابية، يتعيّن أن توفر بيئة التطبيقات SaaS آليات تساعد شريك الخدمة السحابية في التأكد من أن شفراتها أو مكوّناتها الأخرى المورّدة لمورّد الخدمة السحابية تمتثل لأيِّ قيود على البرمجة يفرضها مورد الخدمة السحابية، كما أنه ينبغي ألاَّ تتضمن الشفرات أو المكونات أي برمجيات ضارة وألاَّ تنتهك سلامة الخدمات السحابية لمورّد الخدمة السحابية.

3.3.8 إمكانية صيانة البرمجيات

عندما يكون شريك الخدمة السحابية مطوّر برمجيات سحابية، يتعيّن أن توفر بيئة التطبيقات SaaS آليات تساعد شريك الخدمة السحابية على توفير شفرات مصدر أو جوانب وظيفية أخرى لنظام مورّد الخدمة السحابية. ومن الضروري أن تتضمن شفرات المصدر أو الجوانب الوظيفية طرائق تحديد الإصدار أو أيِّ طرائق أخرى مناسبة، من أجل كفالة إمكانية صيانتها خلال مدة خدمتها. وتشمل هذه الطرائق على سبيل الذكر وليس الحصر، توفير تحديثات لإصلاح مواطِن الضعف المعروفة وإلغاء الاعتماد على المكوّنات الأخرى ذات مواطن الضعف المعروفة وزيادة أمن النظام ككل.

بيبليوغرافيا

[b-ITU-T X.1601] التوصية ITU-T X.1601 (2014)، *إطار أمني للحوسبة السحابية*.

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

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