الاتحـــــــــــاد الدولـــــــــــي للاتصـــــــــــالات

ITU-T

قطاع تقييس الاتصالات
في الاتحاد الدولي للاتصالات

X.1369

(2022/01)

السلسلة X: شبكات البيانات والاتصالات بين الأنظمة المفتوحة ومسائل الأمن

التطبيقات والخدمات الآمنة (2) – أمن إنترنت الأشياء (IoT)

المتطلبات الأمنية لمنصة خدمة إنترنت الأشياء

التوصية ITU-T X.1369

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
القياس الحيوي عن بُعد	X.1099–X.1080
تطبيقات وخدمات آمنة (1)	
أمن البث المتعدد	X.1109–X.1100
أمن الشبكة المحلية	X.1119–X.1110
أمن الخدمات المتنقلة	X.1139–X.1120
أمن الويب (1)	X.1149–X.1140
بروتوكولات الأمن (1)	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 (2)	
اتصالات الطوارئ	X.1309–X.1300
أمن شبكات المحاسيس واسعة الانتشار	X.1319–X.1310
أمن شبكة الكهرباء الذكية	X.1339–X.1330
البريد المعتمد	X.1349–X.1340
أمن إنترنت الأشياء (IoT)	**X.1369–X.1350**
أمن أنظمة النقل الذكية (ITS)	X.1399–X.1370
أمن سجل الحسابات الموزع	X.1429–X.1400
أمن التطبيقات (2)	X.1459–X.1450
أمن شبكة الويب (2)	X.1489–X.1470
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
الدفاع السيبراني	X.1599–X.1590
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
الاتصالات الكمومية	
المصطلحات	X.1701–X.1700
مولّد الأعداد العشوائية الكمومية	X.1709–X.1702
إطار أمن شبكات توزيع المفاتيح الكمومية	X.1711–X.1710
تصميم أمن شبكات توزيع المفاتيح الكمومية	X.1719–X.1712
تقنيات أمن شبكات توزيع المفاتيح الكمومية	X.1729–X.1720
أمن البيانات	
أمن البيانات الضخمة	X.1759–X.1750
حماية البيانات	X.1789–X.1770
أمن شبكات الاتصالات المتنقلة الدولية–2020	X.1819–X.1800

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

التوصية ITU-T X.1369

المتطلبات الأمنية لمنصة خدمة إنترنت الأشياء

ملخص

تحدد التوصية ITU-T X.1369 المتطلبات الأمنية لمنصة خدمة إنترنت الأشياء. وتقيّم التهديدات والتحديات الأمنية التي تواجهها منصة خدمة أعمال إنترنت الأشياء وتصف التدابير الأمنية التي يمكن أن تخفف من التهديدات والتحديات الأمنية.

التسلسل التاريخي

الطبعة	التوصية	تاريخ الموافقة	لجنة الدراسات	معرف الهوية الفريد*
1.0	ITU-T X.1369	2022-01-07	17	11.1002/1000/14799

مصطلحات أساسية

إنترنت الأشياء (LoT)، منصة خدمة، متطلبات أمنية، مخاطر أمنية.

* للنفاذ إلى توصية، ترجى كتابة العنوان http://handle.itu.int/ في حقل العنوان في متصفح الويب لديكم، متبوعاً بمعرف التوصية الفريد. ومثال ذلك، http://handle.itu.int/11.1002/1000/11830-en.

تمهيد

الاتحاد الدولي للاتصالات وكالة الأمم المتحدة المتخصصة في ميدان الاتصالات وتكنولوجيات المعلومات والاتصالات (ICT). وقطاع تقييس الاتصالات (ITU-T) هو هيئة دائمة في الاتحاد الدولي للاتصالات. وهو مسؤول عن دراسة المسائل التقنية والمسائل المتعلقة بالتشغيل والتعريفة، وإصدار التوصيات بشأنها بغرض تقييس الاتصالات على الصعيد العالمي.

وتحدد الجمعية العالمية لتقييس الاتصالات (WTSA) التي تجتمع مرة كل أربع سنوات المواضيع التي يجب أن تدرسها لجان الدراسات التابعة لقطاع تقييس الاتصالات وأن تُصدر توصيات بشأنها.

وتتم الموافقة على هذه التوصيات وفقاً للإجراء الموضح في القرار 1 الصادر عن الجمعية العالمية لتقييس الاتصالات.

وفي بعض مجالات تكنولوجيا المعلومات التي تقع ضمن اختصاص قطاع تقييس الاتصالات، تُعد المعايير اللازمة على أساس التعاون مع المنظمة الدولية للتوحيد القياسي (ISO) واللجنة الكهرتقنية الدولية (IEC).

ملاحظة

تستخدم كلمة "الإدارة" في هذه التوصية لتدل بصورة موجزة سواء على إدارة اتصالات أو على وكالة تشغيل معترف بها.

والتقيد بهذه التوصية اختياري. غير أنها قد تضم بعض الأحكام الإلزامية (بهدف تأمين قابلية التشغيل البيني والتطبيق مثلاً). ويعتبر التقيّد بهذه التوصية حاصلاً عندما يتم التقيّد بجميع هذه الأحكام الإلزامية. ويستخدم فعل "يلزم" وصيغ ملزمة أخرى مثل فعل "يجب" وصيغها النافية للتعبير عن متطلبات معينة، ولا يعني استعمال هذه الصيغ أن التقيّد بهذه التوصية إلزامي.

حقوق الملكية الفكرية

يسترعي الاتحاد الانتباه إلى أن تطبيق هذه التوصية أو تنفيذها قد يستلزم استعمال حق من حقوق الملكية الفكرية. ولا يتخذ الاتحاد أي موقف من القرائن المتعلقة بحقوق الملكية الفكرية أو صلاحيتها أو نطاق تطبيقها سواء طالب بها عضو من أعضاء الاتحاد أو طرف آخر لا تشمله عملية إعداد التوصيات.

وعند الموافقة على هذه التوصية، لم يكن الاتحاد قد تلقى إخطاراً بملكية فكرية تحميها براءات 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.1369

المتطلبات الأمنية لمنصة خدمة إنترنت الأشياء

1 مجال التطبيق

توصف هذه التوصية المتطلبات الأمنية لمنصة خدمة إنترنت الأشياء. وهي تقيّم التهديدات والتحديات الأمنية التي تواجهها منصة خدمة إنترنت الأشياء وتصف التدابير الأمنية التي يمكن أن تخفف من التهديدات والتحديات الأمنية.

2 المراجع

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

[ISO/IEC 30141] ISO/IEC 30141:2018، *Internet of Things Reference Architecture*.

3 التعاريف

1.3 مصطلحات معرَّفة في وثائق أخرى

تستعمل هذه التوصية المصطلح التالي المعرف في وثائق أخرى:

1.1.3 إنترنت الأشياء (Internet of things) (IoT) [ITU-T Y.4000]: بنية تحتية عالمية لمجتمع المعلومات، تمكّن الخدمات المتطورة عن طريق التوصيل البيني للأشياء (المادية والافتراضية) استناداً إلى تكنولوجيات المعلومات والاتصالات القابلة للتشغيل البيني القائمة والمتطورة.

2.3 المصطلحات المعرَّفة في هذه التوصية

تعرِّف هذه التوصية المصطلح التالي:

1.2.3 منصة خدمة إنترنت الأشياء (IoT Service Platform): منصة نظام تُوصل بها أجهزة إنترنت الأشياء وتُنفذ فيها تطبيقاتها.

من منظور وظيفي، توفر منصة خدمة إنترنت الأشياء إمكانات إدارة الأجهزة وإدارة التوصيل وتمكين التطبيق وتحليل الأعمال وما إلى ذلك. ومن منظور إدارة البيانات، تقوم منصة خدمة إنترنت الأشياء بجمع وتخزين ومعالجة البيانات (بما في ذلك البيانات الشخصية والمعلومات السرية للمستعملين) لتطبيقات إنترنت الأشياء والتحليل المتقدم.

4 الاختصارات والأسماء المختصرة

تستخدم هذه التوصية الاختصارات والأسماء المختصرة التالية:

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

CSRF طلب مزوَّر عابر للموقع *(Cross Site Request Forgery)*

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

DoS رفض الخدمة *(Denial of Service)*

IMEI الهوية الدولية للمعدات المتنقلة *(International Mobile Equipment Identity)*

PVLAN شبكة محلية افتراضية خاصة *(Private VLAN)*

SIM وحدة تعرّف هوية المشترك *(Subscriber Identity Module)*

SQL لغة استعلام مبنية *(Structured Query Language)*

SSRF طلب مزور من جانب المخدِّم *(Server Side Request Forgery)*

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

VM آلة افتراضية *(Virtual Machine)*

VMM مرقاب آلة افتراضية *(Virtual Machine Monitor)*

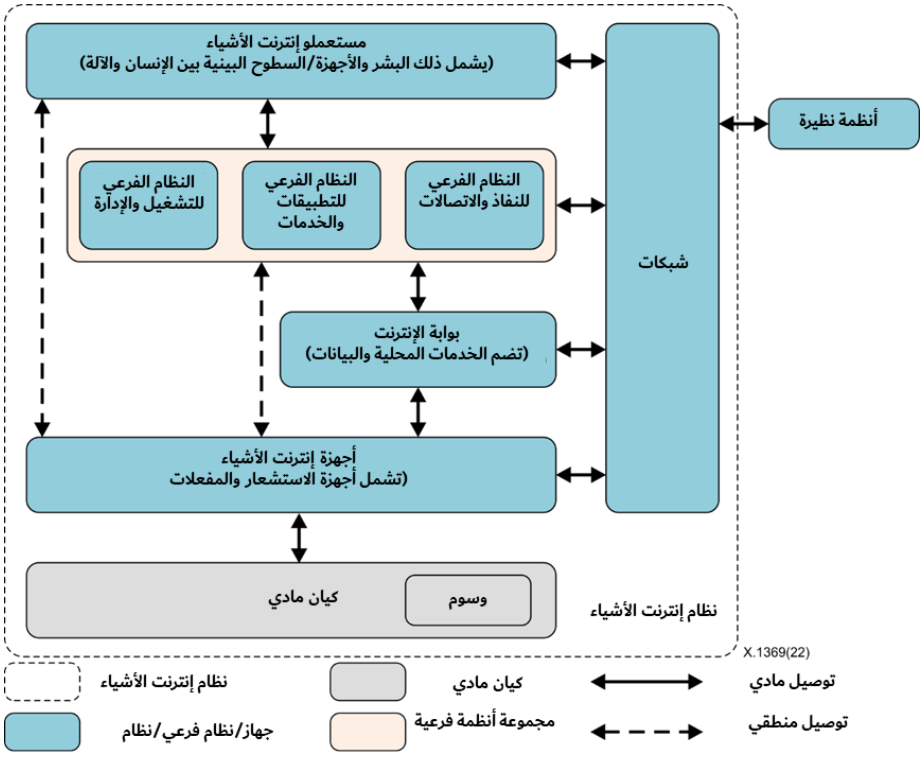
XSS شفرة مندسة عبر مواقع إلكترونية *(Cross Site Script)*

5 الاصطلاحات

تشير الكلمة الرئيسية "**ينبغي**" إلى متطلبٍ "يتعين" الالتزام الصارم به ولا يسمح بالحيْد عنه، في حال زعم الامتثال لهذه التوصية.

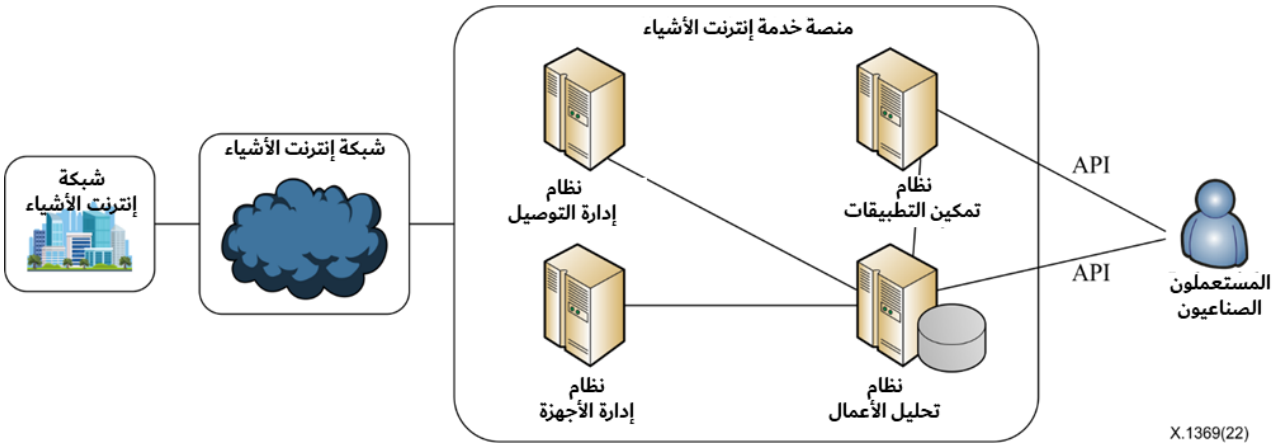
6 نظرة عامة

يعرف المعيار [ISO/IEC 30141] النموذج المرجعي لإنترنت الأشياء المستند إلى الكيان كما هو موضح في الشكل 1. وتعد منصة خدمة إنترنت الأشياء من المكونات الرئيسية *للنظام الفرعي للتطبيقات والخدمات* المبينة في هذا الشكل، والذي يوفر إمكانات مثل إدارة الأجهزة وإدارة التوصيلات وتمكين التطبيقات وتحليل الخدمات. وتقوم منصة خدمة إنترنت الأشياء أيضاً بجمع البيانات وتخزينها وتحليلها لتطبيقات إنترنت الأشياء.



الشكل 1 – النموذج المرجعي لإنترنت الأشياء المستند إلى الكيان (ISO/IEC 30141)

وبشكل عام، يمكن تقسيم منصة خدمة إنترنت الأشياء إلى أربعة أجزاء، تشمل نظام إدارة الأجهزة ونظام إدارة التوصيلية ونظام تمكين التطبيقات ونظام تحليل الأعمال.



الشكل 2 – نظرة عامة على منصة خدمة إنترنت الأشياء

- نظام إدارة الأجهزة

هذا هو نظام إدارة أجهزة إنترنت الأشياء. وهو يوفر وظائف المراقبة عن بعد وإعادة التشكيل وترقية البرمجيات وترقية النظام والكشف عن الأعطال وإصلاحها وإدارة دورة الحياة ووظائف أخرى.

- نظام إدارة التوصيلية

هذا هو نظام الإدارة المركزي لبطاقة وحدة تعرّف هوية المشترك (SIM). وهو يركز على تطبيقات الشبكات الخلوية ويمكن المستخدم من الخدمة الذاتية، مثل الاستعلام عن استخدام البيانات وحالة التوصيل وإعادة شحن البطاقة SIM وإدارة الحركة.

- نظام تمكين التطبيقات

هذا هو منصة من النمط منصة كخدمة يوفر وظائف مختلفة للسطوح البينية لبرمجة التطبيقات (API) لدعم تنفيذ أنظمة الخدمات المختلفة. ومع هذا النظام، يفتح مشغلو الاتصالات قدرات الاتصالات الأساسية الخاصة بهم (البيانات، والرسائل القصيرة، والهاتف، والاستيقان، والفوترة، وما إلى ذلك) لأنظمة الخدمات المختلفة، مثل النقل الذكي، والمدن الذكية، والمنازل الذكية، وما إلى ذلك.

- نظام تحليل الأعمال

هذا يجمع البيانات المختلفة من نظام إدارة الأجهزة ونظام إدارة التوصيلية ونظام تمكين التطبيقات لتحليل وإعداد نتائج التحليل المرئي للمشغلين والمستهلكين.

ولأمن منصة خدمة إنترنت الأشياء دور هام في بيئة إنترنت الأشياء بأكملها. فأي ضعف أو هجوم على المنصة سيؤثر على أمن الأجهزة والشبكات والبيانات ذات الصلة. وتكون منصة خدمة إنترنت الأشياء عرضة للتهديدات بما في ذلك رفض الخدمة وزيادة الامتيازات والنفاذ غير المخول والهجمات الكاسحة وتنفيذ شفرات عشوائية وما إلى ذلك، مما قد يؤدي إلى اختراقات ضارة وتسريب معلومات حساسة وتعليمات خبيثة للأجهزة وعواقب وخيمة أخرى.

وفي هذه التوصية، يتم تحليل المخاطر الأمنية لمنصة خدمة إنترنت الأشياء. وتُطرح منهجية الإطار الأمني والتدابير الأمنية.

ويغطي أمن منصة خدمة إنترنت الأشياء أمن البنية التحتية وأمن النظام وأمن البيانات وأمن التطبيقات من المستوى الأدنى إلى المستوى الأعلى. وإلى جانب ذلك، يتضمن أمن السطوح البينية لبرمجة التطبيقات والأمن التشغيلي المستويات الأربعة. وفي الفقرات من 7 إلى 9، يتم تفصيل المخاطر الأمنية والإطار الأمني والمتطلبات الأمنية على التوالي بناءً على تلك الجوانب الستة.

7 التهديدات الأمنية لمنصة خدمة إنترنت الأشياء

1.7 تهديدات أمن التطبيقات

تشمل تهديدات أمن التطبيقات هجمات الويب والنفاذ غير المخول وزيادة الامتيازات ونقاط ضعف الخدمات وما إلى ذلك.

1.1.7 هجمات الويب

تستخدم منصة خدمة إنترنت الأشياء تكنولوجيات الويب التقليدية بالإضافة إلى تكنولوجيا الاتصالات والبيانات الضخمة والحوسبة السحابية وما إلى ذلك. ونتيجةً لذلك، فإنها تتوارث المخاطر الأمنية الرئيسية لجميع هذه التكنولوجيات، مثل هجمات رفض الخدمة الموزع (DDoS)، والهجمات الكاسحة، ودس لغة الاستعلام البنيوية (SQL)، ومواطن الضعف الخاصة بالشفرات المندسة عبر مواقع إلكترونية (XSS)، ومواطن الضعف المتعلقة بالطلبات المزوَّرة العابرة للموقع (CSRF)، ومواطن الضعف المتعلقة بالطلبات المزورة من جانب المخدِّم (SSRF)، إلخ.

2.1.7 النفاذ وزيادة الامتيازات بدون تخويل

يتم نشر عدد كبير من تطبيقات إنترنت الأشياء في المنصة المركزية. وهذا يجعل من الصعب فصل الأمن بكفاءة والتحكم في النفاذ بين التطبيقات المختلفة، مما قد يؤدي إلى النفاذ والتشغيل وزيادة الامتيازات بدون تخويل. إلى جانب ذلك، فهي تكون عرضة النفاذ وزيادة الامتيازات بدون تخويل بين مختلف المستعملين والأجهزة.

3.1.7 مواطن ضعف الخدمات

تحتوي تطبيقات إنترنت الأشياء على منطق خدمات معقد وعدد كبير من بروتوكولات التطبيقات، وهو ما قد يدخل عيوباً أثناء عمليتي التصميم والتنفيذ مؤدياً إلى ظهور مواطن ضعف الخدمات وإساءة استعمالها. وفي بعض سيناريوهات تطبيقات إنترنت الأشياء، يمكن التحكم في المطاريف من خلال المنصة. وسينتج عن المنصة المخترقة إصابة عدد كبير من المطاريف بالخلل، والتأثير بشكل أكبر على التصنيع الصناعي والحياة الاجتماعية للمستعملين.

4.1.7 عرض القدرات

بوصفها منصة لتمكين التطبيقات، يمكن لمنصة إنترنت الأشياء أن توفر سطوح بينية لبرمجة التطبيقات لوظائف مختلفة لدعم تنفيذ أنظمة الخدمات المختلفة. ويلائم ذلك الخدمات المختلفة، لكن فتح القدرات قد يجلب أيضاً مخاطر للمنصة. وقد يتم النفاذ إلى القدرات من قبل مطورين غير مخولين أو إساءة استخدامها من قبل خدمات مختلفة. علاوةً على ذلك، قد يؤدي فتح قدرات الاتصالات الأساسية (البيانات، والرسائل القصيرة، والهاتف، والاستيقان، والفوترة، وما إلى ذلك) إلى حدوث هجمات على شبكة الاتصالات الأساسية إذا لم تُوفر لها الحماية المناسبة.

2.7 مخاطر أمن البيانات

تشكل سرية البيانات وسلامتها وتيسرها الأساس لأمن البيانات. ومع ذلك، فهناك العديد من المخاطر التي تبرز أثناء عملية جمع البيانات ونقلها وترحيلها وتخزينها ومعالجتها وإتلافها.

1.2.7 تسرب البيانات

عادةً ما يتم جمع بيانات تطبيقات إنترنت الأشياء بواسطة مطاريف إنترنت الأشياء ونقلها إلى المنصة. وعادة ما يتم تخزين بيانات هذه التطبيقات في المنصة. لذلك، يمكن للخصم استخراج البيانات إذا لم تكن محمية بشكل مناسب، وذلك عن طريق هجمات دس اللغة SQL، وهجمات فيض الدارئ، وزيادة الامتيازات، وما إلى ذلك.

2.2.7 التلاعب بالبيانات

يمكن التلاعب بالبيانات أو إعادة تشغيلها أو تعديلها أثناء نقلها. فأثناء عملية نقل بيانات التطبيقات وتخزينها، يكون الخصم قادراً على التلاعب بالبيانات إذا لم تتم حماية البيانات بشكلٍ مناسب. فعلى سبيل المثال، يمكن لخصم إعادة تشغيل المعلومات المستخدمة أو تزوير معلومات مزيفة وإرسال المعلومات إلى منصة إنترنت الأشياء إذا لم تُراع سلامة البيانات أثناء نقلها.

3.7 مخاطر أمن النظام

1.3.7 الإخلال بالحسابات

إذا لم تكن حسابات مديري نظام تشغيل منصة خدمة إنترنت الأشياء معقدة بدرجة كافية، أو إذا كان منفذ غير الضروري للنظام مفتوحاً، فقد يتم الإخلال بالحسابات بهجمة كاسحة وبالمراقبة وما إلى ذلك. كما يهدد التحكم غير السليم في النفاذ أمن النظام.

2.3.7 إساءة استعمال الامتيازات

تعمل خدمات إنترنت الأشياء التي تقدمها المنصة على نظام التشغيل والبرمجيات الوسيطة. فإذا لم يتم تحديث نظام التشغيل أو البرمجيات الوسيطة في الوقت المناسب، فهناك مخاطر تتمثل في أن النظام ذا الإصدار القديم أو البرمجيات الوسيطة ذات الإصدارات القديمة تكون بها به مواطن ضعف يمكن أن يستغلها قراصنة الحاسوب، مما يؤدي إلى زيادة الامتيازات.

4.7 المخاطر الأمنية للبنية التحتية

تكون البنية التحتية عرضة لمخاطر تهدد الأمن المادي وأمن الشبكة والأمن الافتراضي وأمن المعدات.

1.4.7 التهديدات المادية

تؤثر البيئة المادية لمنصة إنترنت الأشياء أيضاً على الأمن. فهي عرضة، على سبيل المثال، لتهديدات طبيعية مثل الزلازل والفيضانات والعواصف والأعاصير وما إلى ذلك. بالإضافة إلى ذلك، يمكن أن تشكل المرافق مثل أنظمة الطاقة والتبريد وحتى أنظمة الأمن نفسها تهديداً لمنصة إنترنت الأشياء. علاوة على ذلك، يجب أيضاً مراعاة العوامل البشرية، والتي قد تتضمن التدمير المتعمد والسرقة والتفجير وما إلى ذلك.

2.4.7 التهديد للشبكة

قد يقوم المهاجمون بتصفح الإنترنت للعثور على نقاط نفاذ إلى منصات خدمة إنترنت الأشياء. وقد يؤدي الافتقار إلى عزل الشبكة بالنسبة لمنصات الخدمة إلى النفاذ إلى البيانات عبر خدمات مختلفة.

3.4.7 المخاطر الافتراضية

حسنت تكنولوجيا المحاكاة الافتراضية للمخدِّم بشكل كبير من كفاءة البناء والمرونة التشغيلية والفوائد الاقتصادية لمنصة إنترنت الأشياء، ولكنها جلبت في نفس الوقت مخاطر جديدة. فعلى سبيل المثال، تسمح عيوب تصميم مرقاب الآلة الافتراضية (VMM) للمهاجمين بالتطفل على مضيف omtp الافتراضي، ومشاركة بطاقة الشبكة مع الآلة الافتراضية لنفس المضيف مما يسهل من انتشار مشاكل الأمن. هناك أيضاً نوع آخر من المخاطر مثل قفزات الآلة الافتراضية (VM) وهجمات رفض الخدمة ومواطن ضعف منصة الإدارة عن بُعد.

5.7 المخاطر الأمنية للسطوح البينية

تتضمن السطوح البينية لمنصة خدمة إنترنت الأشياء السطح البيني للويب والسطح البيني لبرمجة تطبيقات الطرف الثالث والسطح البيني لبرمجة تطبيقات البائع الخلفي، والتي تواجه مخاطر تسرب المعلومات والبرمجة العابرة للمواقع وضعف الاستيقان وضعف التحكم في النفاذ.

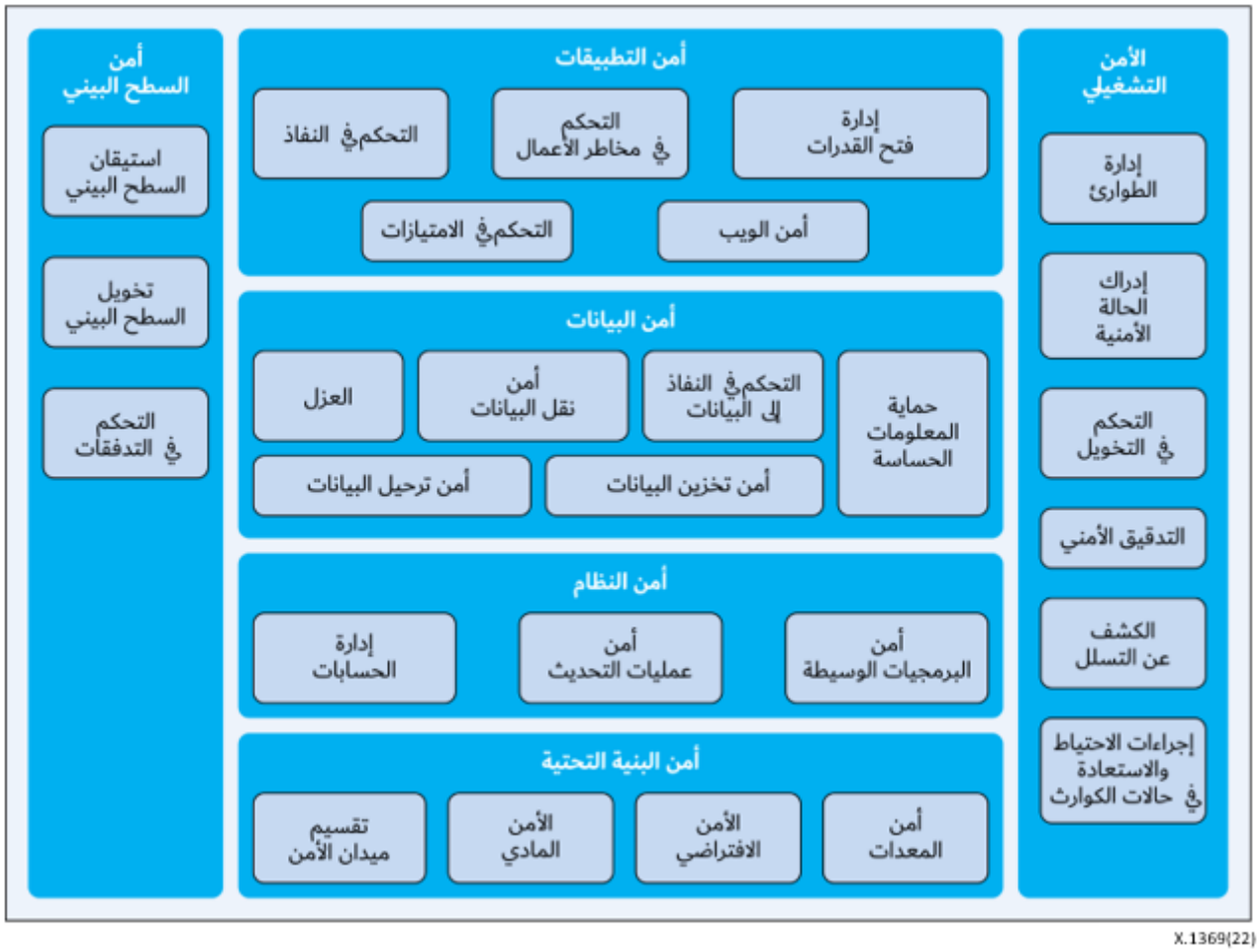
6.7 المخاطر الأمنية التشغيلية

قد تنقطع الخدمة، أثناء التشغيل والصيانة، بسبب الإجراءات التشغيلية غير السليمة للعمليات ولموظفي التشغيل والصيانة. فعلى سبيل المثال، قد يستخدم الموظفون قرص ذاكرة USB مصاباً ببرمجيات ضارة أو قد يحذف البيانات عن طريق الخطأ. وينبغي أيضاً مراعاة التوصيل غير الطبيعي وكلمات المرور المفترضة والهجمات الخبيثة وآليات التدقيق.

8 معمارية أمن منصة خدمة إنترنت الأشياء

تركز معمارية أمن منصة خدمة إنترنت الأشياء على ستة جوانب من متطلبات الحماية الأمنية: أمن التطبيقات وأمن السطوح البينية وأمن البيانات وأمن النظام وأمن البنية التحتية والأمن التشغيلي.

وتُعرض في الشكل 3 معمارية الأمن الشاملة:



الشكل 3 – معمارية أمن منصة خدمة إنترنت الأشياء

1.8 أمن التطبيقات

يشمل أمن التطبيقات التحكم في النفاذ، والتحكم في الامتيازات، والتحكم في مخاطر الأعمال، وأمن الويب وإدارة عرض القدرات، والتي من شأنها أن تساعد على حل مشكلات زيادة الامتيازات، والنفاذ غير المخول، وما إلى ذلك.

2.8 أمن البيانات

يشمل أمن البيانات أمن عزل البيانات ونقلها والتحكم في النفاذ وأمن تخزين البيانات، وهو ما من شأنه أن يؤدي إلى حل مشكلة تسرب الخصوصية ومشكلات أمن البيانات الأخرى.

3.8 أمن النظام

يشمل أمن النظام إدارة الحسابات وأمن تحديث البرمجيات وأمن البرمجيات الوسيطة، وهو ما من شأنه أن يساعد في حل مشكلات الاستخدام الضار للثغرات الأمنية المعروفة.

4.8 أمن البنية التحتية

يشمل أمن البنية التحتية تقسيم الميدان الأمني، والأمن المادي، والأمن المرئي، وأمن المعدات، وهو ما من شأنه أن يؤدي إلى حل مشكلات الاستخدام الضار للثغرات الأمنية المعروفة.

5.8 أمن السطوح البينية

يشمل السطوح البينية استيقان السطح البيني، وتخويل السطح البيني، والتحكم في التدفقات، وهو ما من شأنه أن يساعد في حل مشكلات انتهاكات المعلومات المحددة لهوية الأشخاص، وحقن اللغة SQL، وما إلى ذلك.

6.8 الأمن التشغيلي

يشمل الأمن التشغيلي إدارة الطوارئ، والتوعية بالحالة الأمنية، والتحكم في التخويل، والتدقيق الأمني، وكشف التسلل، والنسخ الاحتياطي والتعافي في حالات الكوارث، مما يساعد على حل المشكلات المتعلقة بالأمن التشغيلي.

9 المتطلبات الأمنية لمنصة خدمة إنترنت الأشياء

1.9 أمن التطبيقات

ينبغي أن تكون منصة الخدمة قادرة على منع الهجمات من الإنترنت على الحدود، خاصة الهجمات على البيانات الضخمة والحوسبة السحابية وتطبيقات الويب وغيرها من التكنولوجيات. وينبغي توفير القدرة على منع هجمات رفض الخدمة الموزع والعبث والتسلل والفيروسات لضمان التشغيل الآمن والمستقر لمنصة الخدمة.

1.1.9 التحكم في النفاذ

1.1.1.9 التحكم في نفاذ المستعمل

1) ينبغي إنشاء نظام تعرف هوية المستعمل لتخصيص وسم هوية فريد لكل مستعمل الذي ينبغي أن يظل كما هو حتى إذا قام المستعمل بتغيير رقم الهاتف المحمول وصندوق البريد أو غير ذلك من المعلومات.

2) ينبغي نشر الكشف عن كلمات المرور الضعيفة بشكلٍ دوري. بالإضافة إلى ذلك، يجب تجفير كلمة المرور أثناء عملية الإرسال. وبالنسبة للخدمات ذات المستويات العالية من الأمن، ينبغي النظر في آلية الاستبدال الدوري الإلزامي لكلمة المرور.

3) ينبغي التعامل مع استخدام الرسائل القصيرة الدينامية بشكل صارم. وينبغي اعتماد تدابير أمنية مثل التحقق من الخلفية، والإلغاء الفوري بعد الاستخدام، والحد من عدد عمليات تسجيل الدخول الخاطئة، ومنع الاستيقان المحلي، وما إلى ذلك.

4) ينبغي استخدام آلية شفرة الاستيقان البيانية في سيناريو تسجيل الدخول. ويجب مراعاة تدابير التخليط في الخلفية مثل ضوضاء الخلفية، وعدم استخدام النظام الإثنيني، ومكافحة التجزئة، والخط المباشر، وتشويه دوران الخط، وما إلى ذلك، لمنع التعرف السريع على الآلة.

5) ينبغي أن تتمتع المنصة بقدرات التحكم في المخاطر ومقاومة التصادم. وينبغي أن تكون لديها القدرة على تحديد النفاذ الشرعي. فعلى سبيل المثال، ينبغي منع الفك العنيف لكلمات المرور بالتقييد العددي لعمليات تسجيل الدخول الفاشلة، وعنوان IP، ومعرف هوية الجهاز، ووقت القفل، وأسلوب الفتح، وفي نفس الوقت عبر الإنترنت.

6) أثناء عملية إعادة تحديد كلمة المرور واستعادتها، ينبغي التحقق من الهوية بدقة لمنع تجاوز الاستيقان وتزوير الهوية.

2.1.1.9 التحكم في نفاذ التطبيق

1) إنشاء نظام لتعرف هوية التطبيقات وتخصيص معرف هوية فريد لكل تطبيق.

2) ينبغي الاستيقان من صلاحية التطبيق الذي ينفذ إلى المنصة. وينبغي عدم السماح إلا للتطبيق المستيقن منه بالنفاذ إلى منصة الخدمة لتنفيذ استدعاءات الخدمة اللاحقة.

3) يحظر نقل المفاتيح في نص غير مشفر أو تطبيق تحويل لخوارزميات ضعيفة (مثل MD5) للمفاتيح أثناء عملية استيقان التطبيق.

4) ينبغي تخصيص مفاتيح مختلفة للتطبيقات المختلفة، كما ينبغي دعم وظائف إدارة المفاتيح لإنشاء المفاتيح وتوزيعها وتخزينها وتحديثها.

5) ينبغي استيقان استدعاء السطوح البينية للحد من نطاق الموارد والسلطة التشغيلية التي يمكن تشغيلها.

3.1.1.9 التحكم في نفاذ الجهاز

1) ينبغي إنشاء نظام لتعرف هوية الجهاز. يخصص معرف هوية فريد لكل جهاز IoT وربط المعرف بمعلومات المعدات المقابلة، مثل الشركة المصنعة للجهاز، ونوع الجهاز، والقالب، وما إلى ذلك.

2) تخصيص مفتاح جهاز فريد لكل جهاز من خلال نظام التوزيع المسبق للمفاتيح، ونظام تبادل المفاتيح، وما إلى ذلك. وينبغي ربط مفتاح الجهاز ومعرف هوية الجهاز معاً. وينبغي دعم وظائف إدارة المفاتيح لإنشاء المفاتيح وتوزيعها وتخزينها وتحديثها.

3) تطبيق استيقان الهوية عند نفاذ الجهاز إلى المنصة. وينبغي عدم السماح إلا للجهاز المستيقن منه بالنفاذ إلى منصة الخدمة لعمليات الخدمة اللاحقة.

4) يحظر نقل المفاتيح في نص غير مشفر أو تطبيق تحويل لخوارزميات ضعيفة (مثل MD5) للمفاتيح أثناء عملية استيقان التطبيق.

2.1.9 التحكم في الامتيازات

1) ينبغي دعم إدارة تصنيف المستعملين وتجميعهم. وينبغي منح الامتيازات المختلفة وفقاً لتصنيفات المستعملين ومجموعاتهم المختلفة. وينبغي عدم السماح إلا للمستعملين المخولين بالنفاذ إلى البيانات المحددة وإجراء العمليات المقابلة.

2) ينبغي منح الامتيازات المختلفة وفقاً لتصنيفات التطبيقات المختلفة. وينبغي عدم السماح إلا للتطبيقات المخولة باستدعاء قدرات الخدمة المحددة وتنفيذ العمليات المقابلة.

3) ينبغي منح الامتيازات المختلفة وفقاً لأنواع أو تصنيفات الأجهزة المختلفة. وينبغي عدم السماح إلا للأجهزة المخول لها بالنفاذ إلى البيانات والمعلومات المحددة وتنفيذ العمليات المقابلة.

3.1.9 التحكم في مخاطر الأعمال

1.3.1.9 إدارة أمن بطاقات إنترنت الأشياء والتحكم فيه

ينبغي التقييد الصارم لوظائف الاتصالات الخاصة ببطاقات إنترنت الأشياء لأنواع الخدمات المختلفة بناءً على مبدأ "الحد الأدنى، والضروري، والقابل للتحكم". فعلى سبيل المثال، ينبغي إبقاء وظيفة الصوت والرسائل القصيرة أحادية الاتجاه في بعض السيناريوهات، وينبغي تقييد وظيفة البيانات عندما يكون تدفق البيانات غير طبيعي.

2.3.1.9 إدارة أمن الخدمات والتحكم فيه

ينبغي أن يتسنى الحد من إجمالي كمية تدفقات البيانات ووتيرتها، والرسائل القصيرة، والصوت، وما إلى ذلك، وإغلاق الخدمة عند تجاوز العتبة المحددة.

3.3.1.9 التحكم في سلوك المستعمل

ينبغي تقييد إجمالي كمية التدفقات والوتيرة والوقت الذي ينفذ فيه المستعملون إلى المنصة. وعندما يتصرف المستعملون تصرفاً غير اعتيادي، يجب إيقاف النفاذ على الفور.

4.3.1.9 مراقبة شرود الأجهزة

ينبغي مراقبة سلوك الأجهزة. وعند اكتشاف سلوك غير طبيعي للجهاز (على سبيل المثال، وقت غير مناسب، وزيارات غير مناسبة، ومنطقة موقع غير اعتيادية)، ينبغي توفير آلية إنذار ومعالجة.

5.3.1.9 مراقبة مخاطر الخدمات

ينبغي تحليل بيانات مطاريف إنترنت الأشياء في أبعاد متعددة مثل المقدار الإجمالي والتدفق الأقصى، وذلك لاكتشاف خلل تشغيل الخدمة في الوقت المناسب. وأثناء تشغيل الخدمة، ينبغي أيضاً مراقبة إساءة استخدام الخدمة. فعلى سبيل المثال، يمكن اكتشاف انقسام الجهاز والبطاقة من خلال مراقبة أرقام الهوية الدولية للمعدات المتنقلة. وفي الوقت نفسه، يمكن تعزيز القدرة على اكتشاف المخاطر الأمنية وتحليلها والقضاء عليها من وجهة نظر شاملة، باستخدام البيانات الضخمة التي تم جمعها من تشغيل المطاريف.

4.1.9 أمن الويب

1) ينبغي توفير قدرة قوية لمكافحة الهجمات DDOS، وينبغي تكييف استراتيجيات لمكافحة الهجمات DDOS (على سبيل المثال، تدفق الحركة وتنظيف الحركة على الشبكة وما إلى ذلك) لطبقة التطبيق وطبقة الشبكة.
2) ينبغي أن يحتوي المنصة على إمكانية فحص ثغرات الويب، والتي يمكنها اكتشاف ومنع المشكلات الأمنية مثل تحميل الملفات، ودس لغة SQL، وثغرات الشفرات المندسة XSS، والثغرات الخاصة بالطلبات CSRF والطلبات SSRF.
3) ينبغي أن يكون لدى المنصة القدرة على فحص الثغرات الأمنية للمضيف والعثور على نقاط الضعف في نظام المعلومات، بما في ذلك الثغرات الأمنية ومشاكل التشكيلة الأمنية ونقاط الضعف الأمنية لنظام التطبيق وكلمات المرور الضعيفة.
4) ينبغي أن يكون لدى المنصة القدرة على تقييد وقت توصيل قاعدة البيانات والنفاذ إلى الشبكة في تطبيقات الويب لتجنب الاستهلاك غير الضروري للموارد.
5) ينبغي أن يكون لدى المنصة القدرة على اكتشاف التسلل، وتسجيل عنوان IP للمصدر، ونوع الهجوم، والغرض من الهجوم، وتوقيت الهجوم الخاص بالتسلل، وإطلاق إنذار عند حدوث تسلل خطير.

5.1.9 إدارة عرض القدرات

1.5.1.9 استيقان الهوية

ينبغي أن يدعم نظام تمكين التطبيقات استيقان الهوية. فعندما يطلب المطور بعض وظائف السطح البيني لبرمجة التطبيقات وينفذها، ينبغي استيقان شرعية المطورين والتطبيقات، وينبغي عدم تزوير هوية المطورين الشرعيين والتطبيقات الشرعية.

2.5.1.9 تعزيز التطبيقات وحمايتها

ينبغي أن يكون لنظام تمكين التطبيقات وظيفة لتعزيز وحماية التطبيقات التي تستدعي وظائف السطوح البينية API، لمنع العبث بالتطبيق وتفكيكه.

3.5.1.9 حماية أمن البيانات

ينبغي أن يضمن نظام تمكين التطبيقات سرية وسلامة المعلومات الحساسة المتعلقة بالحسابات والإثباتات الخاصة بالمستعملين والتطبيقات، لمنع سرقة المعلومات أو العبث بها أثناء التخزين والنقل والاستخدام. فعلى سبيل المثال، ينبغي تجفير المعلومات الحساسة المنقولة بين تطبيقات إنترنت الأشياء والمنصة، وينبغي مراعاة حماية السلامة، وضمان عدم كشف المعلومات الحساسة للكيانات وعمليات المعالجة غير المخولة، أو تعديلها أو إتلافها أو إعادة تشغيلها بواسطتها، إلخ.

4.5.1.9 استيقان استدعاء القدرات

ينبغي أن يدعم نظام تمكين التطبيقات استيقان وتخويل استدعاء القدرات. فعندما يستدعي التطبيق القدرة، ينبغي استيقان الوتيرة والمقدار الإجمالي ونوع القدرات التي يمكن للمطور والتطبيق استدعاءها. ولا ينبغي استدعاء القدرات إلا بعد التخويل.

5.5.1.9 مراقبة استدعاء القدرات

ينبغي أن يدعم نظام تمكين التطبيقات مراقبة الوتيرة والوقت والمقدار الإجمالي لاستدعاء القدرات. وعند تجاوز الحد أو كان السلوك غير اعتيادي، ينبغي إيقاف الوظيفة فوراً وإطلاق إنذار في نفس الوقت.

2.9 أمن البيانات

ينبغي أن تحمي المنصة البيانات خلال دورة حياتها بأكملها، بما في ذلك التخزين والنقل والاستخدام، وما إلى ذلك. وينبغي النسخ الاحتياطي لبيانات الخدمات الحرجة بشكل دوري، وينبغي تشكيل آلية استعادة لضمان سرية البيانات وسلامتها وتيسرها.

1.2.9 عزل البيانات

ينبغي تنفيذ البيانات المختلفة وحفظها في بيئات معزولة. وينبغي أن يكون بوسع المنصة عزل المعلومات الحساسة بشكل منطقي والتحكم في التفاعلات بين الحقول المختلفة بشكل صارم.

2.2.9 أمن نقل البيانات

1) ينبغي حماية المعلومات الحساسة المنقولة بين منصة الخدمة وأجهزة إنترنت الأشياء ومنصات الخدمات الأخرى (بما في ذلك كلمة مرور المدير المسؤول عن الخلفية وكلمة مرور تسجيل الدخول إلى نظام التشغيل وكلمة مرور تسجيل الدخول إلى جهاز الشبكة وإجابات حماية كلمة المرور المرتبطة بكلمات المرور هذه) بشكل سري.
2) ينبغي حماية سلامة المعلومات الحساسة بين منصات الخدمات وأجهزة إنترنت الأشياء ومنصات الخدمات الأخرى.

3.2.9 التحكم في النفاذ

ينبغي أن تدعم المنصة وظيفة التحكم في النفاذ، فعلى سبيل المثال، ينبغي تحديد سياسات النفاذ المختلفة لقاعدة البيانات لأنظمة المحاكاة الافتراضية المختلفة لضمان ألا يتمكن المستعملون من العمل إلا في إطار تخويل قاعدة البيانات لنظام الخدمة المقابل وألا يتمكنوا من النفاذ إلى بيانات أنظمة خدمة أخرى غير مخول لها.

4.2.9 أمن تخزين البيانات

1) ينبغي تصنيف البيانات حسب أهميتها، واعتماد آليات مختلفة حسب مستوى تصنيف البيانات. فعلى سبيل المثال، يمكن تخزين البيانات الأقل أهمية في نص غير مشفر، مع ضمان سرية البيانات المهمة.
2) ينبغي أن توفر المنصة آلية تخزين آمنة للمفاتيح. فمثلاً، يتم تخزين المفاتيح داخل آلة التجفير أو وكيل معين لضمان عدم تسريب المفاتيح.
3) ينبغي حماية سلامة البيانات. وينبغي توفير آلية للكشف عن سلامة البيانات الحساسة للغاية، بحيث يمكن الكشف عن تلف هذه البيانات وفقدانها في الوقت المناسب. وتتضمن البيانات الحساسة للغاية اسم المستعمل ورقم الحساب وما إلى ذلك.
4) ينبغي أن توفر المنصة آلية نسخ احتياطي واستعادة للبيانات. وفي حال فقد البيانات أو تدميرها، ينبغي استخدام آلية النسخ الاحتياطي لاستعادة البيانات لضمان عدم فقدانها بعد وقوع الحوادث.
5) ينبغي أن تتمتع المنصة بالقدرة على أرشفة جميع أنواع البيانات والملفات ووظيفة لتنظيف البيانات والملفات المؤقتة بشكلٍ أوتوماتي ودوري.
6) ينبغي تحرير مساحة لتخزين الملفات والأدلة وقواعد البيانات في النظام أو إعادة توزيعها، بحيث تكون قابلة للإلغاء التام وغير قابلة للاسترداد.

3.9 أمن النظام

ينبغي للنظام الذي تستخدمه المنصة أن يأخذ في الاعتبار أمن إدارة الحسابات وتحديث البرمجيات وأمن البرمجيات الوسيطة، وهو ما من شأنه أن يساعد على حل مشكلات الاستخدام الضار لنقاط الضعف المعروفة.

1.3.9 إدارة الحسابات

1) ينبغي لنظام المنصة أن يقوم بتسجيل سجلات النظام أوتوماتياً، مثل معلومات تسجيل دخول المستعملين ومعلومات التشغيل وما إلى ذلك.

2) بالنسبة للأنظمة التي تتم صيانتها عن بُعد بواسطة بروتوكول HTTP، ينبغي أن يدعم النظام بروتوكولات التجفير مثل البروتوكول HTTPS.

3) بالنسبة للنظام الذي يحتوي على السطح البيني للأحرف، ينبغي أن يدعم الخروج الأوتوماتي لحساب التوقيت.

4) ينبغي أن يأخذ النظام في الاعتبار التحكم في النفاذ إلى موارد المضيف، على سبيل المثال، لإنشاء نموذج يحتذى به ووضع سياسة أمن مناسبة للتحكم في الدور المختلف لنفاذ المستعملين إلى موارد المضيف.

2.3.9 أمن تحديث البرمجيات

1) ينبغي تحديث إصدار/التصحيحات الأمنية لنظام التشغيل في الوقت المناسب.

2) ينبغي عدم السماح إلا بتثبيت المكونات والتطبيقات المطلوبة فقط.

3) ينبغي أن يفتح النظام المنافذ الضرورية فقط ويغلق المنافذ غير الضرورية.

3.3.9 أمن البرمجيات الوسيطة

1) ينبغي تحديث الإصدار/التصحيحات الأمنية للبرمجيات الوسيطة في الوقت المناسب.

2) ينبغي تعطيل السطوح البينية للبرمجيات الوسيطة غير الضرورية لمنع تسرب معلومات النظام.

3) ينبغي حماية علم البرمجية الوسيطة (اسم البرمجية/عنوان رقم الإصدار) لمنع تسرب معلومات النظام.

4.9 أمن البنية التحتية

ينبغي أن يأخذ أمن البنية التحتية في الاعتبار تقسيم الميدان الأمني، والأمن المادي، والأمن المرئي، وأمن المعدات، وهو ما من شأنه أن يؤدي إلى حل مشكلات الاستخدام الضار لنقاط الضعف المعروفة.

1.4.9 تقسيم الميدان الأمني للشبكة

1) ينبغي تقسيم الميادين الأمنية بين منصات الخدمة والإنترنت، وبين منصات الخدمة وأنظمة الدعم الداخلية، وبين أنظمة الخدمات المختلفة المستضافة داخل المنصة. وينبغي تقسيم حدود الميادين الأمنية بين الميادين الأخرى وميدان النفاذ، وبين ميدان النفاذ والميدان الأساسي وداخل الميدان الأساسي.

2) ينبغي تقسيم أنظمة الخدمات المختلفة في منصة الخدمة إلى شبكات محلية افتراضية (VLAN) مختلفة، وينبغي أن تستخدم الميادين الأمنية المختلفة مقاطع مختلفة من الشبكة VLAN. وينبغي أن تستخدم أنظمة الخدمة المختلفة في كل ميدان أمني شبكات محلية افتراضية مختلفة، ويتم عزل جميع الشبكات المحلية الافتراضية بالتغيب. وفي الشبكة VLAN نفسها، ينبغي دعم عزل الآلة الافتراضية (VM) على مستويات أمنية مختلفة لنفس نظام الخدمة، مثل تقسيم الشبكة VLAN الفرعية بواسطة تكنولوجيا الشبكات VLAN الخاصة (PVLAN).

3) ينبغي اعتماد سياسة نفاذ متبادل. فعلى سبيل المثال، تُنفذ تشكيلة استراتيجية للنفاذ المتبادل للميادين الأمنية المختلفة داخل نظام الخدمة، والنفاذ المتبادل بين أنظمة الخدمات المختلفة.

4) ينبغي دعم وظيفة عزل الميدان الأمني. فعلى سبيل المثال، يمكن تقسيم شبكة المنصة إلى ميدان للإدارة وميدان للخدمة وميدان للسطح البيني وما إلى ذلك. وينبغي توزيع الأجهزة ذات الوظائف المختلفة على ميادين أمنية مختلفة. وينبغي تنفيذ كشف التسلل والتحكم في النفاذ على حدود الميادين الأمنية.

2.4.9 الأمن المادي

1) ينبغي أن تفي البيئة المادية بمتطلبات حماية السلامة للموقع، وإمدادات الطاقة، والحرائق، والكتامة المائية، ومكافحة الشحنات الاستاتيكية، والتحكم في درجة الحرارة والرطوبة.

3.4.9 الأمن الافتراضي

1) ينبغي أن تدعم المنصة حماية المشرف على الآلات الافتراضية وعزل الآلة الافتراضية، وتعزيز نظام المضيف السحابي، ومراقبة أمن الآلة الافتراضية، والحماية من البرمجيات الضارة، والتحكم في التطبيقات، وغيرها من الوظائف لتجنب مشكلات أمن التمثيل الافتراضي الشائعة.

4.4.9 أمن المعدات

1) ينبغي أن تفي المرافق المادية بمتطلبات التشكيلة الأساسية لحماية السلامة ومتطلبات الاختبار. وينبغي توفير الحوسبة الموثوقة لتعزيز أمن المرافق.

5.9 أمن السطوح البينية

يشمل السطوح البينية استيقان السطح البيني، وتخويل السطح البيني، والتحكم في التدفقات، وهو ما من شأنه أن يساعد في حل مشكلات انتهاكات المعلومات المحددة لهوية الأشخاص، وحقن اللغة SQL، وما إلى ذلك.

1.5.9 استيقان السطح البيني

1) ينبغي أن يكون للمنصة القدرة على التحقق من الشرعية بين أنظمة الخدمة، وذلك لمنع استخدام المنصة والنفاذ إليها بدون تخويل.

2) ينبغي أن يكون لمنصة الخدمة وظيفة تسجيل سجل العمليات الكامل للموارد التي تم استدعاؤها.

2.5.9 تخويل السطح البيني

1) ينبغي أن يكون لمنصة الخدمة وظيفة التخويل وفقاً لمدى عناوين IP للمصدر. فبالإضافة إلى توفير كلمة مرور ثابتة، تحتاج منصة الخدمة التي تم استدعاؤها أيضاً إلى تخويل مدى عناوين IP.

2) بالنسبة للسطوح البينية التي تتطلب حقوق نفاذ المستعمل، ينبغي وجود آلية نفاذ لرفض/السماح بقائمة لاعتراض نفاذ مستعمل غير شرعي.

3.5.9 التحكم في التدفقات

1) ينبغي أن تتمتع المنصة بالقدرة على التحكم في معدل التدفقات من خلال تحديد سياسة التحكم في التدفقات، ويمكن تعديل قيمة التشكيلة في السياسة وفقاً لضبط أداء مخدم السطح البيني API في الطرف الخلفي. وعندما يتجاوز عدد الطلبات المتزامنة الحد، يتم رفض الطلبات الزائدة ويُعاد رد خطأ.

6.9 الأمن التشغيلي

يشمل الأمن التشغيلي إدارة الطوارئ، والتوعية بالحالة الأمنية، والتحكم في التخويل، والتدقيق الأمني، وكشف التسلل، والنسخ الاحتياطي والتعافي في حالات الكوارث، مما يساعد على حل المشكلات المتعلقة بالأمن التشغيلي.

1.6.9 إدارة الطوارئ

1) ينبغي أن تنشئ المنصة آلية للاستجابة لحوادث الطوارئ، مثل حوادث الأمن السيبراني، وحوادث السلامة في مكان العمل، وما إلى ذلك.

2) تُعقد تدريبات الطوارئ بانتظام ويتم إنشاء نظام للتمارين المنتظمة على خطط الطوارئ.

2.6.9 التوعية بالحالة الأمنية

1) يوصى بإنشاء نظام للتوعية بالحالة الأمنية لتحقيق المراقبة والتقييم والإنذار المبكر والتصور والاستجابة المركزية للوضع الأمني للمنصة، وذلك للتحسين الفعال لمراقبة التهديدات الأمنية للشبكة والتوعية بالموقف والاستجابة للطوارئ والتعقب وغير ذلك من القدرات، وتحسين كفاءة التشغيل الأمني والصيانة الأمنية.

3.6.9 التحكم في التخويل

1) ينبغي أن تقوم المنصة بإجراء الاستيقان والتخويل الضروريين للعمليات المختلفة للمنصة. وللحصول على امتيازات عالية المستوى، يمكن فقط لموظفي النظام الموثوق بهم إجراء عمليات الامتيازات عالية المستوى.

2) ينبغي للمنصة إنشاء نماذج يحتذى بها، والتحكم في نفاذ المستعملين إلى موارد المضيف وفقاً للسياسات الأمنية.

4.6.9 التدقيق الأمني

1) ينبغي تسجيل جميع عمليات المديرين ووضعها في صورة في سجل.

2) عندما تشارف سعة التخزين على النفاذ، ينبغي ضمان عدم فقدان سجل التدقيق.

3) ينبغي النسخ الاحتياطي لسجلات التدقيق.

4) ينبغي تحصين سجلات التدقيق من عمليات النفاذ والتعديل والتدمير غير المخولة.

5) ينبغي تصدير سجلات التدقيق وحذفها.

6) ينبغي النفاذ إلى السجلات بطريقة آمنة لضمان سرية وسلامة عملية النقل.

7) ينبغي أن تتمتع المنصة بوظائف المراقبة في الوقت الفعلي والتدقيق الدوري للسلوكيات غير المعتادة مثل التوصيل غير الاعتيادي والنفاذ غير الاعتيادي والتطبيق غير الاعتيادي بناءً على تحليل الحركة ومراجعة السجل والبيئات التجريبية وما إلى ذلك، وينبغي الإنذار والتخلص في الوقت المناسب طبقاً للسلوك غير الاعتيادي المكتشف.

5.6.9 كشف التسلل

1) ينبغي أن تنشر المنصة معدات لكشف التسلل لكشف أي تسلل في الوقت المناسب.

6.6.9 النسخ الاحتياطي والتعافي في حالات الكوارث

1) في حالات الحرائق والزلازل والكوارث الأخرى، ينبغي أن تكون المنصة قادرة على التبديل إلى نظام النظام الاحتياطي المتكرر البعيد في الوقت المناسب لمواصلة خدمتها.

2) ينبغي أن تدعم المنصة استعادة البيانات الحساسة بعد الكوارث (مثل بيانات الخدمة، وبيانات الفوترة، وبيانات تشكيلة النظام، وسجلات التشغيل والصيانة للمديرين، ومعلومات المستعملين، وما إلى ذلك) للتأكد من أنه عند حذف البيانات الهامة بشكلٍ ضار، يمكن للنظام التعافي في الوقت المناسب.

بيبليوغرافيا

[b-ITU-T X.1361] Recommendation ITU-T X.1361 (2018), *Security framework for the Internet of things based on the gateway model*.

[b-ITU-T X.1362] Recommendation ITU-T X.1362 (2017), *Simple encryption procedure for Internet of things (IoT) environments*.

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

[b-ITU-T Y.4000] Recommendation ITU-T Y.4000/Y.2060 (2012), *Overview of the Internet of things.*

[b-ITU-T Y.4100] Recommendation ITU-T Y.4100/Y.2066 (2014), *Common requirements of the Internet of things*.

سلاسل التوصيات الصادرة عن قطاع تقييس الاتصالات

السلسلة A	تنظيم العمل في قطاع تقييس الاتصالات
السلسلة D	مبادئ التعريفة والمحاسبة والقضايا الاقتصادية والسياساتية المتصلة بالاتصالات/تكنولوجيا المعلومات والاتصالات على الصعيد الدولي
السلسلة E	التشغيل العام للشبكة والخدمة الهاتفية وتشغيل الخدمات والعوامل البشرية
السلسلة F	خدمات الاتصالات غير الهاتفية
السلسلة G	أنظمة الإرسال ووسائطه والأنظمة والشبكات الرقمية
السلسلة H	الأنظمة السمعية المرئية والأنظمة متعددة الوسائط
السلسلة I	الشبكة الرقمية متكاملة الخدمات
السلسلة J	الشبكات الكبلية وإرسال إشارات تلفزيونية وبرامج صوتية وإشارات أخرى متعددة الوسائط
السلسلة K	الحماية من التداخلات
السلسلة L	البيئة وتكنولوجيا المعلومات والاتصالات، وتغير المناخ، والمخلفات الإلكترونية، وكفاءة استخدام الطاقة، وإنشاء الكبلات وغيرها من عناصر المنشآت الخارجية وتركيبها وحمايتها
السلسلة M	إدارة الاتصالات بما في ذلك شبكة إدارة الاتصالات وصيانة الشبكات
السلسلة N	الصيانة: الدارات الدولية لإرسال البرامج الإذاعية الصوتية والتلفزيونية
السلسلة O	مواصفات تجهيزات القياس
السلسلة P	نوعية الإرسال الهاتفي والمنشآت الهاتفية وشبكات الخطوط المحلية
السلسلة Q	التبديل والتشوير، والقياسات والاختبارات المرتبطة بهما
السلسلة R	الإرسال البرقي
السلسلة S	التجهيزات المطرافية للخدمات البرقية
السلسلة T	المطاريف الخاصة بالخدمات التليماتية
السلسلة U	التبديل البرقي
السلسلة V	اتصالات البيانات على الشبكة الهاتفية
السلسلة X	**شبكات البيانات والاتصالات بين الأنظمة المفتوحة ومسائل الأمن**
السلسلة Y	البنية التحتية العالمية للمعلومات، والجوانب الخاصة ببروتوكول الإنترنت وشبكات الجيل التالي وإنترنت الأشياء والمدن الذكية
السلسلة Z	اللغات والجوانب العامة للبرمجيات في أنظمة الاتصالات

طُبعت في سويسرا
جنيف، 2022