الاتحـــــــــــاد الدولـــــــــــي للاتصـــــــــــالات

ITU-T

قطاع تقييس الاتصالات
في الاتحاد الدولي للاتصالات

X.1752

(2022/01)

السلسلة X: شبكات البيانات والاتصالات بين الأنظمة المفتوحة ومسائل الأمن

أمن البيانات – أمن البيانات الضخمة

مبادئ توجيهية بشأن أمن البنية التحتية للبيانات الضخمة ومنصتها

التوصية ITU-T X.1752

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 (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
أمن التطبيقات (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 تكنولوجيا السجلات الموزعة (DLT)	X.1429–X.1400
أمن التطبيقات (2)	X.1459–X.1450
أمن الويب (2)	X.1489–X.1470
تبادل معلومات الأمن السيبراني	
نظرة عامة عن الأمن السيبراني	X.1519–X.1500
تبادل المعلومات عن مواطن الضعف/الحالة	X.1539–X.1520
تبادل المعلومات عن الأحداث/الأحداث العارضة/المعلومات الحدسية	X.1549–X.1540
تبادل المعلومات عن 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.1752

مبادئ توجيهية بشأن أمن البنية التحتية للبيانات الضخمة ومنصتها

ملخص

تحلل التوصية ITU-T X.1752 التهديدات والتحديات الأمنية التي تواجهها البنية التحتية للبيانات الضخمة ومنصتها وتحدد إطاراً مرجعياً لإقامة التقابل بين المبادئ التوجيهية الأمنية والتهديدات التي تواجهها البنية التحتية للبيانات الضخمة ومنصتها.

التسلسل التاريخي

الطبعة	التوصية	تاريخ الموافقة	لجنة الدراسات	معرف الهوية الفريد*
1.0	ITU-T X.1752	2022-01-07	17	11.1002/1000/14806

مصطلحات أساسية

البيانات الضخمة، البنية التحتية، المنصة، مبادئ توجيهية 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.1752

مبادئ توجيهية بشأن أمن البنية التحتية للبيانات الضخمة ومنصتها

1 مجال التطبيق

تصف هذه التوصية البنية التحتية للبيانات الضخمة ومنصتها من منظور أعمال التقييس الحالية في المنتديات ذات الصلة. وتحدد هذه التوصية منهجية لتقييم التهديدات كما تحدد مبادئ توجيهية أمنية لحماية البنية التحتية للبيانات الضخمة ومنصتها. وتوفر هذه التوصية أيضاً تقابلاً بين التهديدات والمبادئ التوجيهية الأمنية.

2 المراجع

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

[ITU-T X.1279] التوصية ITU-T X.1279 (2020)، *إطار للاستيقان المعزز باستخدام القياسات البيومترية عن بُعد مع آليات الكشف عن حالات الانتحال*.

[ITU-T X.1601] التوصية ITU-T X.1601 (2015)، *إطار الأمن للحوسبة السحابية*.

[ITU-T X.1603] التوصية ITU-T X.1603 (2018)، *متطلّبات أمن البيانات لخدمة مراقبة الحوسبة السحابية*.

[ITU-T X.1605] التوصية ITU-T X.1605 (2020)، *متطلبات أمن البنية التحتية كخدمة (IaaS) عمومية في الحوسبة السحابية*.

[ITU-T Y.3600] التوصية ITU-T Y.3600 (2015)، *البيانات الضخمة – متطلبات وإمكانات قائمة على الحوسبة السحابية*.

[ITU-T Y.3605] التوصية ITU-T Y.3605 (2020)، *البيانات الضخمة – المعمارية المرجعية*.

3 التعاريف

1.3 مصطلحات معرَّفة في مصادر أخرى

تعرِّف هذه التوصية المصطلحات التالية المعرَّفة في وثائق أخرى:

1.1.3 التحكم في النفاذ (access control) [b-ITU-T X.800]: منع استخدام غير مرخص به لمورد ما، بما في ذلك منع استخدام مورد بطريقة غير مرخص بها.

2.1.3 التدقيق (audit) [b-ITU-T X.800]: استعراض مستقل وفحص لسجلات النظام وأنشطته بغية اختبار مدى كفاية ضوابط النظام، ولضمان الامتثال للسياسات والإجراءات التشغيلية المعمول بها، ولكشف الخروقات الأمنية، وللتوصية بأي تغييرات ضرورية في الضوابط والسياسات والإجراءات.

3.1.3 الاستيقان (authentication) [b-ISO/IEC 18014-2]: تقديم ضمان يؤكد هوية كيان ما.

4.1.3 تحليل البيانات الضخمة (big data analysis) [b- ITU-T Y.2244]: تدقيق يُجرى على حجم ضخم من البيانات بغرض الحصول على نتائج ذات مغزى، مثل الاتجاهات أو التفضيلات.

5.1.3 إزالة حساسية البيانات (data desensitization) [b-ITU-T X.1217]: عملية لإخفاء البيانات الحساسة.

6.1.3 سلامة البيانات (data integrity) [b-ITU-T X.800]: خاصية بقاء البيانات على حالتها دون أن يطرأ عليها تغيير أو تلف بطريقة غير مرخص بها.

7.1.3 جدار الحماية (firewall) [b-ISO/IEC 27033-1]: نوع من الحواجز الأمنية يوضع بين البيئات الشبكية. يتألف من جهاز مكرس أو مجموعة من العديد من المكونات والتقنيات – تمر من خلاله كل الحركة العابرة من بيئة شبكية لأخرى، والعكس، ولا يسمح بمرور إلا الحركة المخوَّلة التي تحددها السياسات الأمنية المحلية.

8.1.3 موازنة الحمل (load balancing) [b-ITU-T Y.2052]: مخطط يمكن من خلاله فصل حمل الحركة وموازنته للاستفادة الفعالة من موارد الشبكة (على سبيل المثال، عرض نطاق الوصلة).

9.1.3 نظام كشف الاقتحام (intrusion detection system) [b-ISO/IEC 27039]: أنظمة معلومات تستخدم للكشف عن محاولة اقتحام أو عن الاقتحام أثناء حدوثه أو بعد حدوثه.

10.1.3 نظام منع الاقتحام (intrusion prevention system) [b-ITU-T X.1361]: شكل من أشكال أنظمة كشف الاقتحام مصمم خصيصاً لتوفير القدرة على الاستجابة النشطة.

11.1.3 الاستيقان متعدد العوامل (multi-factor authentication) [b-ITU-T X.1158]: استيقان يدخل فيه على الأقل عاملان مستقلان للاستيقان.

12.1.3 التكرار (redundancy) [b-ITU-T E.800]: في عنصر ما، وجود أكثر من وسيلة لأداء الوظيفة المطلوبة.

13.1.3 المتانة (robustness) [b-ITU-T J.1014]: خاصية تنفيذ وظيفة أمنية للسطح البيني ECI تمثل الجهود و/أو التكلفة التي ينطوي عليها إلحاق الضرر بأمن الوظيفة الأمنية المنفذة.

14.1.3 معلمات التشكيلة الأمنية (security configuration parameter) [b-ITU-T X.1046]: مجموعة من المعلمات التي تصف سمات وظيفة الأمن، مثل الحد الأقصى لعرض النطاق، والحد الأقصى لعدد التوصيلات، وما إلى ذلك، التي تدعمها وظيفة الأمن، والكائن المحمي وإجراءات الأمن الخاصة بوظيفة الأمن.

15.1.3 تسجيل دخول وحيد (single sign-on) [b-ITU-T Y.2201]: القدرة على استعمال استيقان مؤكد من مشغل شبكة/مورد خدمة إلى مشغل/مورد آخر بالنسبة لمستعمل ما لدى نفاذه إلى خدمة ما أو لدى التجوال في شبكة مزارة.

16.1.3 التهديد (threat) [b-ISO/IEC 27000]: سبب محتمل لحادث غير مرغوب قد يُلحق ضرراً بالنظام أو المنظمة.

17.1.3 التحقق (validation) [b-ITU-T Z.450]: عملية فحص مواصفة ما للتأكد من أنها سليمة تركيبياً ودلالياً وتمثل السلوك المقصود.

18.1.3 نقطة التعرض (vulnerability) [b-ITU-T X.1524]: أي موطن ضعف في البرمجية يمكن استغلاله لانتهاك حرمة نظام ما أو المعلومات التي يتضمنها.

19.1.3 القائمة البيضاء (whitelist) [b-ITU-T X.1245]: قائمة تحدد هويات أشخاص أو مصادر تستعمل خدمات الاتصالات، وهي معرفة أو موثوقة أو مسموحة علنياً.

2.3 المصطلحات المعرَّفة في هذه التوصية

تعرّف هذه التوصية المصطلحين التاليين:

1.2.3 البنية التحتية للبيانات الضخمة (big data infrastructure): نظام يضم الأجهزة المادية الأساسية وبيئة الشبكة في النظام الإيكولوجي للبيانات الضخمة لأداء خدمات البيانات الضخمة لجمع البيانات ومعالجة البيانات وإدارة البيانات وما إلى ذلك.

2.2.3 منصة البيانات الضخمة (Big data platform): نظام أو مجموعة من الأنظمة الموزعة في النظام الإيكولوجي للبيانات الضخمة لإجراء وظائف تحليل البيانات والتمثيل المرئي للبيانات ووظائف أخرى.

4 الاختصارات والأسماء المختصرة

تستخدم هذه التوصية الاختصارات والأسماء المختصرة التالية:

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

BDAP مورد تطبيقات البيانات الضخمة *(Big Data Application Provider)*

BDIP مورد البنية التحتية للبيانات الضخمة *(Big Data Infrastructure Provider)*

DOS رفض الخدمة *(Denial of Service)*

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

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

IDS نظام كشف الاقتحام *(Intrusion Detection System)*

IP بروتوكول الإنترنت *(Internet Protocol)*

IPS نظام منع الاقتحام *(Intrusion Prevention System)*

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

VM آلة افتراضية *(Virtual Machine)*

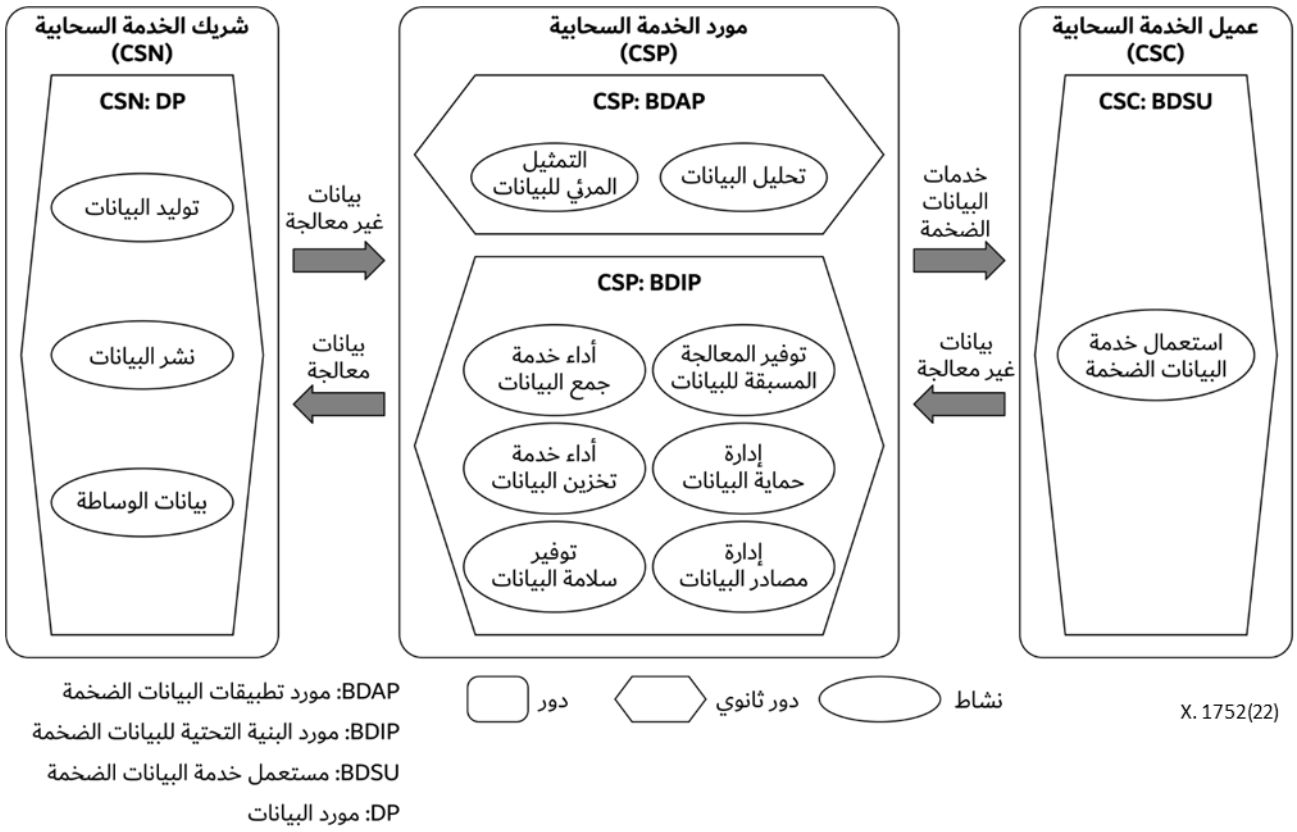
5 الاصطلاحات

في هذه التوصية:

"**يوصى**" كلمة تدل على متطلب يوصى به لكنه غير إلزامي إطلاقاً.

6 التهديدات والتحديات الأمنية التي تواجهها البنية التحتية للبيانات الضخمة ومنصتها

على النحو المحدد في التوصية [ITU-T Y.3600] والموضح في الشكل 6-1 (أي، على النحو المكيَّف من الشكل 7-1 من التوصية [ITU-T Y.3600])، يوفر مورد تطبيقات البيانات الضخمة (BDAP) منصة البيانات الضخمة لإجراء وظائف تحليل البيانات والتمثيل المرئي للبيانات ووظائف أخرى. ويوفر مورد البنية التحتية للبيانات الضخمة (BDIP) البنية التحتية للبيانات الضخمة لأداء خدمات البيانات الضخمة بما في ذلك جمع البيانات ومعالجة البيانات وإدارة البيانات وما إلى ذلك.



الشكل 6-1 – نظام بيانات ضخمة قائم على الحوسبة السحابية

1.6 التهديدات والتحديات الأمنية التي تواجهها البنية التحتية للبيانات الضخمة

تشمل التهديدات والتحديات الأمنية التي تواجهها البنية التحتية للبيانات الضخمة تلك المتعلقة بجمع البيانات وتخزين البيانات وتكامل البيانات والمعالجة المسبقة للبيانات وإدارة البيانات.

1.1.6 التهديدات والتحديات الأمنية المتعلقة بجمع البيانات

فيما يتعلق بأمن جمع البيانات، تشمل التهديدات والتحديات الأمنية ما يلي:

أ) جمع البيانات دون تخويل: يمكن أن يقوم مهاجمون بجمع بيانات دون إذن المستعمل أو تخويله.

ب) موطن ضعف في السطح البيني لجمع البيانات: قد يستخدم المهاجمون موطن ضعف في السطح البيني لجمع البيانات للنفاذ إلى عملية التجميع والتسبب في فقدان البيانات.

ج) نفاذ الإدارة غير المخوَّل به: يمكن لنفاذ الإدارة غير المخوَّل به إلى نظام جمع البيانات أن يؤدي إلى فقدان البيانات. فعلى سبيل المثال، قد يستغل مهاجمون موطن ضعف في النظام للحصول على نفاذ إدارة غير مخوَّل به إلى نظام جمع البيانات وتعديل عنوان بروتوكول الإنترنت لمقصد جمع البيانات إلى عنوان المهاجمين.

2.1.6 التهديدات والتحديات الأمنية المتعلقة بتخزين البيانات

فيما يتعلق بأمن تخزين البيانات، تشمل التهديدات والتحديات الأمنية ما يلي:

أ) فقدان البيانات وتسربها: قد يسبب غياب الإدارة المناسبة لمعلومات التجفير، مثل مفاتيح التجفير وشفرات الاستيقان وامتيازات النفاذ، أضراراً بالغة مثل فقدان البيانات وتسربها غير المتوقع إلى الخارج. بالإضافة إلى ذلك، فإن التقارب الهائل للبيانات متعددة المصادر يزيد من صعوبة التحكم في النفاذ لتخزين البيانات. وتجعل السيناريوهات المعقدة لتخزين وتدفق البيانات الضخمة تنفيذ تجفير البيانات أمراً صعباً.

ب) عدم تيسر الخدمة: يمكن أن يُهاجَم مخدِّم تخزين البيانات بهجوم رفض الخدمة (DoS) أو هجوم رفض الخدمة الموزَّع (DDoS)؛ وبالإضافة إلى ذلك، يمكن أن يتعطل عتاد تخزين بيانات المراقبة ويتسبب بفقدان البيانات أو إتلافها.

ج) التهديدات والتحديات الأمنية للمرافق المادية لتخزين البيانات: فيما يتعلق بأمن المرافق المادية، فهي تواجه تهديدات وتحديات أمنية مماثلة على النحو المحدد في الفقرة 3.9 في التوصية [ITU-T X.1601] والفقرة 7 في التوصية [ITU-T X.1605].

د) تهديدات وتحديات الخدمة التي يواجهها مطراف تخزين البيانات: فيما يتعلق بمطراف تخزين البيانات، تركز التهديدات والتحديات الأمنية على معلمات التشكيلة الأمنية للأجهزة والبرمجيات الخاصة بالمطاريف التي تتضمن معلمات التشكيلة الأمنية لنظام التشغيل، وبرمجيات المكتب، والمتصفح، ونظام البريد، وما إلى ذلك. وتتضمن التهديدات والتحديات الأمنية الرئيسية مجموعة خاطئة من معلمات التشكيلة الأمنية، والتحديثات المتأخرة لمعلمات التشكيلة الأمنية، ومواطن الضعف في معلمات التشكيلة الأمنية، إلخ.

3.1.6 التهديدات والتحديات الأمنية المتعلقة بتكامل البيانات

فيما يتعلق بأمن تكامل البيانات، تشمل التهديدات والتحديات الأمنية ما يلي:

أ) إساءة استخدام البيانات: يمكن للبيانات أن تنتقل بين مواقع مادية مختلفة أثناء عملية تكامل البيانات. ومن الأهمية بمكان عدم السماح بإساءة استخدام البيانات جراء انتقال البيانات إلى مواقع مختلفة.

ب) الانتحال: كما هو معرف في التوصية [ITU-T X.1279]، هو ادعاء كيان ما بأنه كيان مختلف، بتقديم صورة مسجلة أو عينة بيانات بيومترية أخرى أو خاصية بيومترية مشتقة اصطناعياً، من أجل انتحال شخصية فرد ما. ويمكن لمهاجمين انتحال صفة نظام إدارة أو مخدِّم تخزين البيانات، والتسبب بفقدان البيانات أو سوء استخدامها أثناء عملية تكامل البيانات.

ج) تهديدات أمن الشبكة أثناء عملية تكامل البيانات: تواجه تهديدات وتحديات أمنية مماثلة على النحو المحدد في الفقرة 5.9 في التوصية [ITU-T X.1601]. بالإضافة ذلك، تركز التحديات الأمنية الخاصة في البنية التحتية للبيانات الضخمة على الإدارة المتكاملة للأمن عبر الشبكة المادية والشبكة الافتراضية والبيئات السحابية.

4.1.6 التهديدات والتحديات الأمنية المتعلقة بالمعالجة المسبقة للبيانات

فيما يتعلق بأمن المعالجة المسبقة للبيانات، تشمل التهديدات والتحديات الأمنية ما يلي:

أ) التهديدات الداخلية: قد يسيء الموظف التابع للمورد BDAP استخدام بيانات المستعمل لأغراض أخرى غير المقصودة أثناء المعالجة المسبقة للبيانات دون إذن المستعمل.

ب) موطن ضعف في النظام: يمكن فقدان البيانات أثناء المعالجة المسبقة للبيانات بسبب مواطن ضعف في النظام.

5.1.6 التهديدات والتحديات الأمنية المتعلقة بإدارة البيانات

فيما يتعلق بأمن إدارة البيانات، تشمل التهديدات والتحديات الأمنية ما يلي:

أ) مواطن ضعف البرمجيات: يمكن للمهاجمين استغلال مواطن الضعف الأمنية المحتملة للبرمجيات المستخدمة في إدارة البيانات الضخمة. ويمكن للعيوب التقنية الناتجة عن إضفاء الطابع الافتراضي على النظام أن تتسبب في العديد من المخاطر الأمنية؛ كما أن تكنولوجيات التشغيل والصيانة غير المكتملة يمكن أن تنتج مخاطر أكثر خطورة. بالإضافة إلى ذلك، تتسبب نماذج الحوسبة والتخزين الموزعة واسعة النطاق للبنية التحتية للبيانات الضخمة ومنصتها في مخاطر أكبر لمعلمات التشكيلة الأمنية للبرمجية المستخدمة في إدارة البيانات الضخمة.

ب) انقطاع التحكم في النفاذ: يمكن لانقطاع التحكم في النفاذ إلى إدارة البيانات أن يتسبب في فقدان البيانات أو تسربها أو إساءة استعمالها.

ج) نفاذ الإدارة غير المخوَّل به: يمكن لنفاذ الإدارة غير المخوَّل به إلى نظام إدارة البيانات الضخمة أن يؤدي إلى فقدان البيانات أو تسربها أو إساءة استعمالها. فعلى سبيل المثال، قد يستغل مهاجمون موطن ضعف في النظام للحصول على نفاذ إدارة غير مخوَّل به إلى نظام البيانات الضخمة وتعديل عنوان بروتوكول الإنترنت لمقصد جمع البيانات إلى عنوان المهاجمين.

د) التهديدات الداخلية: وجود مستعملين مهملين أو غير مدربين بالقدر الكافي (أو أفراد العائلة في حالة العميل)، أو الأفعال الخبيثة التي يقوم بها موظفون ناقمون، يمكن أن تتسبب في فقدان البيانات.

2.6 التهديدات والتحديات الأمنية التي تواجه منصة البيانات الضخمة

التهديدات والتحديات الأمنية التي تواجه منصة البيانات الضخمة هي تلك المتعلقة بالتمثيل المرئي للبيانات وتحليل البيانات.

1.2.6 التهديدات والتحديات الأمنية المتعلقة بتحليل البيانات

فيما يتعلق بأمن تحليل البيانات، تشمل التهديدات والتحديات الأمنية ما يلي:

أ) موطن ضعف في النظام: يمكن فقدان البيانات بسبب وجود موطن ضعف في نظام تحليل البيانات.

ب) هجوم رفض الخدمة/رفض الخدمة الموزع: يمكن أن يتعرض مخدِّم تحليل البيانات لهجوم رفض الخدمة/رفض الخدمة الموزع.

ج) الاستخدام المشترك لتطبيقات تحليل البيانات: عادةً ما يتم استخدام تطبيقات تحليل البيانات من قبل مستعملين مختلفين، مما قد يتسبب في هروب الآلة الافتراضية (VM) وتسرب البيانات وما إلى ذلك.

د) النفاذ غير المؤمن: يمكن للنفاذ غير المؤمن إلى تحليل البيانات الضخمة أن يتسبب في فقدان بيانات التطبيق أو تسربها أو إساءة استعمالها.

هـ) نفاذ إدارة غير مخوَّلة: يمكن لنفاذ إدارة غير مخوَّلة إلى تحليل البيانات الضخمة أن يتسبب في فقدان البيانات.

2.2.6 التهديدات والتحديات الأمنية المتعلقة بالتمثيل المرئي للبيانات

فيما يتعلق بأمن التمثيل المرئي للبيانات، تشمل التهديدات والتحديات الأمنية ما يلي:

أ) إساءة استخدام البيانات: يمكن أن يسيء الموردون BDAP استخدام البيانات أثناء التمثيل المرئي للبيانات (أو أن يعرضوها بدون إذن المستعمل).

ب) موطن ضعف في النظام: يمكن فقدان بيانات الإبلاغ والتحليل بسبب موطن ضعف في نظام التمثيل المرئي للبيانات.

ج) التحريف: يمكن تحريف البيانات أثناء التمثيل المرئي للبيانات دون إذن المستعمل نتيجة لخلل في سياسات التحكم في النفاذ.

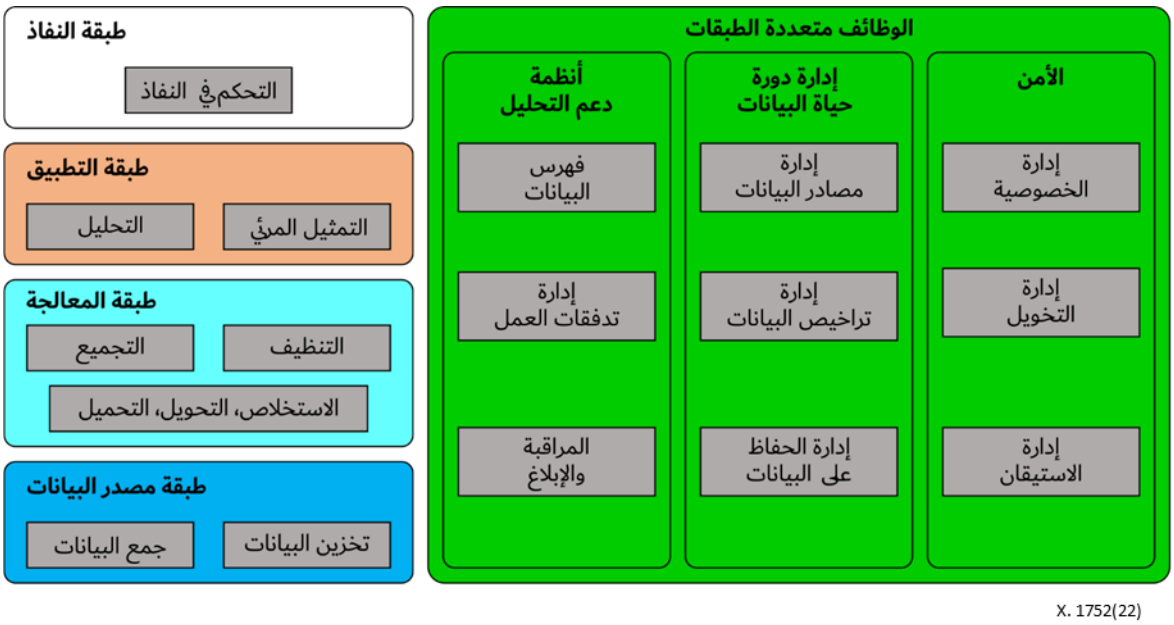
7 مبادئ توجيهية أمنية بشأن البنية التحتية للبيانات الضخمة ومنصتها

كما هو محدد في التوصية [ITU-T Y.3605]، يتكون إطار الطبقات المستخدم في المعمارية المرجعية للبيانات الضخمة من أربع طبقات، بالإضافة إلى مجموعة من الوظائف التي تمتد عبر هذه الطبقات. وهذه الطبقات الأربع هي:

- طبقة النفاذ؛
- طبقة التطبيق؛
- طبقة المعالجة؛
- طبقة مصدر البيانات؛

ويُطلق على الوظائف التي تمتد عبر الطبقات اسم الوظائف متعددة الطبقات.

ويُعرض إطار الطبقات في الشكل 7-1 (أي على النحو المكيَّف من الشكل 8-2 من التوصية [ITU-T Y.3605]).



الشكل 7-1 – إطار طبقات البيانات الضخمة

واستناداً إلى إطار الطبقات الموضح في الشكل 7-1، تستخدم هذه التوصية معمارية لأمن البنية التحتية للبيانات الضخمة ومنصتها كما هو مبين في الشكل 7-2.

الشكل 7-2 – معمارية أمن البنية التحتية للبيانات الضخمة ومنصتها

توصف هذه التوصية المبادئ التوجيهية الأمنية بشأن البنية التحتية للبيانات الضخمة ومنصتها، وتشمل:

أ) مبادئ توجيهية أمنية لطبقة مصدر البيانات؛

ب) مبادئ توجيهية أمنية لطبقة معالجة البيانات؛

ج) مبادئ توجيهية أمنية لطبقة التطبيق؛

د) مبادئ توجيهية أمنية لطبقة النفاذ؛

هـ) مبادئ توجيهية أمنية لإدارة الأمن.

1.7 مبادئ توجيهية أمنية لطبقة مصدر البيانات

تركز المبادئ التوجيهية الأمنية لطبقة مصدر البيانات على أمن البنية التحتية الأساسية وأمن تخزين البيانات.

1.1.7 المبادئ التوجيهية الأمنية للبنية التحتية الأساسية

تشمل المبادئ التوجيهية الأمنية للبنية التحتية الأساسية ما يلي:

أ) يوصى بتقسيم البنى التحتية الافتراضية إلى ميادين أمنية داخلية وخارجية وتنفيذ سياسات أمنية مختلفة عند الطلب. ويوصى بتوفير آليات عزل فعالة بين الميادين الأمنية الداخلية والخارجية.

ب) يوصى بتنفيذ سياسات صارمة للتحكم في النفاذ بين الميادين الأمنية للبنى التحتية الافتراضية. ويوصى باستخدام مبدأ الامتياز الأقل، وبالتالي يتم تخصيص استيقان وتخويل المستعمل على أساس مسؤوليات الأدوار للسماح بالتحكم في النفاذ إلى البنى التحتية الافتراضية.

ج) يوصى بنشر برمجيات أمنية، مثل ببرمجيات مكافحة الفيروسات، في البنى التحتية الافتراضية لتعزيز الحماية الأمنية، وتحديث قواعد بيانات الفيروسات والشفرات الضارة بشكل دوري.

د) يوصى بنشر معدات الكشف عن الهجمات على الشبكة والحماية منها، على سبيل المثال، نظام منع الاقتحام (IPS)/نظام كشف الاقتحام (IDS)، وجدر الحماية، والحماية من الهجمات DDoS وما إلى ذلك، على الحدود بين الشبكات الداخلية والخارجية، وتحديث قواعد بيانات توقيعات الهجمات بشكل دوري إلى آخر الإصدارات.

هـ) يوصى بتنفيذ سياسات صارمة بشأن العزل والتحكم في النفاذ على حدود الشبكات الداخلية والخارجية لمنع عمليات النفاذ غير المخول إلى البنى التحتية الأساسية.

و) يوصى بمراقبة حركات الشبكة للبنى التحتية الأساسية وإجراء عمليات تفتيش متعمقة، بما في ذلك معلومات المفاتيح مثل إحصاءات تدفقات الشبكة وحركة الشبكة غير الاعتيادية وما إلى ذلك.

ز) يوصى بعرض معلومات الهجمات، مثل نوع الهجوم، وعناوين IP للمصدر/المقصد، وخاتم التوقيت وما إلى ذلك عند اكتشاف الهجمات.

ح) يوصى بإجراء مراقبة أمنية مركزية في الوقت الفعلي تشمل حالة تشغيل مختلف الموارد المادية والافتراضية.

2.1.7 المبادئ التوجيهية الأمنية لتخزين البيانات

تشمل المبادئ التوجيهية الأمنية لتخزين البيانات ما يلي:

أ) يوصى بتنفيذ مكونات تخزين مأمونة للبيانات، مثل نظام الملفات الموزعة الآمن، والتخزين المفهرس الآمن، وما إلى ذلك، لضمان أمن بيئة التخزين.

ب) يوصى بدعم استراتيجيات العزل لبيانات المستعملين المختلفين في البيئات متعددة الشاغلين.

ج) يوصى بصياغة سياسات أمنية ولوائح إدارية لتخزين البيانات، مثل سياسة التحكم في النفاذ، وسياسة نقل البيانات الآمنة، وسياسة سلامة البيانات، وسياسة تناسق النسخ المتعددة، والمعلومات الشخصية وسياسة تجفير البيانات الأساسية، وما إلى ذلك.

د) يوصى بدعم مجموعة متنوعة من آليات إزالة حساسية البيانات.

هـ) يوصى بدعم تجفير نظام الملفات، من أجل منع تلف البيانات وتسربها. بالإضافة إلى ذلك، يوصى بدعم عمليات التجفير المصنفة بناءً على مستويات حساسية البيانات: بدون تجفير، تجفير جزئي، تجفير كامل، إلخ.

و) يوصى بتوفير وظائف من أجل الكشف عن الأضرار التي لحقت بسلامة بيانات التخزين واستعادة سلامة البيانات بعد حدوث الأضرار.

ز) يوصى بدعم معلمات التشكيلة الأمنية الاختيارية للتشفير ليختارها المستعملون.

ح) يوصى بدعم المستعملين في اختيار آلية تجفير طرف ثالث لتجفير بيانات المفاتيح.

ط) يوصى بدعم تجفير البيانات باستعمال مفاتيح مؤمنة ودعم التخزين والحفاظ على المفاتيح المؤمنة محلياً.

ي) يوصى بدعم خوارزمية تجفير مناسبة من أجل إعداد النسخ الاحتياطية لوسائط التخزين طويلة الأجل (الأرشيفية)، كاستخدام مفاتيح تجفير طويلة والتخطيط للإحلال بخوارزمية تجفير محسنة.

ك) يوصى بتحديد توقيتات وحقوق مشاركة البيانات، والتخويل باستخدام البيانات وحذف البيانات.

ل) يوصى بترخيص فترة صلاحية استخدام البيانات وإخطار موردي البيانات الضخمة ومستعمليها ذوي الصلة.

م) يوصى بدعم وظائف حذف البيانات والنسخ الاحتياطي والاستعادة.

2.7 المبادئ التوجيهية الأمنية لطبقة المعالجة

تركز المبادئ التوجيهية الأمنية لطبقة المعالجة على أمن تجميع البيانات وأمن تحليل البيانات.

1.2.7 المبادئ التوجيهية الأمنية لتجميع البيانات

تشمل المبادئ التوجيهية الأمنية لتجميع البيانات ما يلي:

أ) يوصى بأن تدعم مكونات تجميع البيانات أن تدعم آلية للاستيقان، ويتعين استيقان وتخويل مطراف مصدر البيانات ومشغلي منصة البيانات الضخمة.

ب) يوصى بتنفيذ لوائح أمنية صارمة في عملية تجميع البيانات، تشمل التصنيف والنقل والتخزين المؤقت.

ج) يوصى بأن تقوم مصادر البيانات المختلفة بوضع استراتيجية تصنيف للبيانات مع سياسة إدارة الأمن المقابلة، والتي ينبغي أن تغطي عملية النقل والتخزين المؤقت. ويوصى بأن يُحدد لكل فئة من فئات مصادر البيانات سياسة إدارة الأمن المقابلة من خلال السرية والسلامة والتيسر.

د) يوصى بدعم وظائف التحكم في النفاذ المقيد للنفاذ إلى مجلد لتخزين مؤقت في عملية تجميع البيانات، كي يمكن حظر النفاذ إلى العمليات غير المرغوب فيها أو بيانات المستعملين، والتعديل غير المخول لعنوان تخزين مكونات تجميع البيانات.

هـ) يوصى بتوفير وظائف موازنة الحمل لمكونات تجميع البيانات، كي يمكن تخفيف ضغط الحمل لتدفقات البيانات الكبيرة بواسطة قنوات متعددة.

و) يوصى بتوفير وظائف الكشف والحماية مثل نظامي IPS/IDS لمكونات تجميع البيانات، بحيث يمكن فرض قيود على الجمع المفرط أو غير المرغوب فيه للبيانات.

ز) يوصى بتوفير آليات لتجاوز الخلل والاستعادة لمكونات تجميع البيانات، كي يمكن تحويل تدفقات البيانات التي يتم نقلها إلى مكون احتياطي.

ح) يوصى بتوفير التسجيل لتجميع البيانات وإطلاق إنذارات في الحالات غير الاعتيادية بما في ذلك: أن يتم جمع بيانات بشكل متكرر، أو أن تكون تدفقات البيانات أكبر من الحد المعين، أو انقطاع تدفق البيانات، أو تجاوز مقدار تخزين البيانات المجمعة.

2.2.7 المبادئ التوجيهية الأمنية لتحليل البيانات

تشمل المبادئ التوجيهية الأمنية لتحليل البيانات ما يلي:

أ) يوصى بتوفير أساليب للاستيقان للتأكد من تمكن المستعملين الشرعيين أو التطبيقات الشرعية فقط من إطلاق طلبات تحليل البيانات.

ب) يوصى بتنفيذ وحدة نمطية للتحكم في النفاذ لتحليل البيانات وفقاً لسياسة تعرف هوية مستعمل البيانات الضخمة وسياسة استيقان المستعمل، بما في ذلك إدارة توقيتات التحكم في النفاذ والتحقق منها، وآلية التحقق من شرعية النفاذ إلى البيانات.

ج) يوصى بدعم التدقيق الأمني لتحليل البيانات الموزعة، والتي يوصى من أجلها بتخزين معلومات التدقيق والتحكم فيها بشكل استباقي.

د) يوصى بتوفير آلية لإزالة الحساسية للحفاظ على أمن ومتانة تحليل البيانات، ويوصى بألا تتأثر استمرارية الأعمال مطلوبة. بالإضافة إلى ذلك، يوصى بألا يتأثر أداء النظام بشكل كبير بعد استخدام آلية إزالة الحساسية.

هـ) يوصى بأن يتسنى تحديد آليات مختلفة لإزالة الحساسية وفقاً لمتطلبات المستعملين المختلفة والبيانات المختلفة.

و) يوصى بدعم تشكيلة خوارزمية إزالة الحساسية بعد استفسار المستعملين أو طلبهم.

ز) يوصى بإمكانية إضافة أو حذف آليات إزالة الحساسية دينامياً، بحيث يمكن دعم الترقية السلسة للنظام دون انقطاع للأعمال.

3.7 المبادئ التوجيهية الأمنية لطبقة التطبيق

تركز المبادئ التوجيهية الأمنية لطبقة التطبيق على نظام التطبيق وتدقيق التطبيق.

1.3.7 المبادئ التوجيهية الأمنية لنظام التطبيق

تشمل المبادئ التوجيهية الأمنية لنظام التطبيق ما يلي:

أ) يوصى بتوفير أساليب للكشف والحماية لنظام التطبيق، مثل جدر الحماية ونظام مكافحة الفيروسات وأنظمة IDS/IPS.

ب) يوصى بتنفيذ دفاعات ضد مواطن ضعف نظام التطبيق.

ج) يوصى بتوفير أساليب للاستيقان لمنع النفاذ غير المخول إلى نظام التطبيق.

د) يوصى بالحفاظ على العزل بين التطبيقات المختلفة، لتجنب تسرب البيانات الناجم عن تحليل ارتباط البيانات الذي تطلقه التطبيقات المختلفة.

2.3.7 المبادئ التوجيهية الأمنية لتدقيق التطبيق

تشمل المبادئ التوجيهية الأمنية لتدقيق التطبيق ما يلي:

أ) يوصى بتدقيق عمليات مديري التطبيقات، بحيث يتسنى تتبع الأحداث واستخراج الأدلة للحوادث الأمنية.

ب) يوصى بتدقيق عمليات مستعملي التطبيقات للتمكين من اكتشاف السلوكيات الضارة والإنذار بها والاستجابة السريعة لها.

ج) يوصى بتدقيق تعديل معلمات التشكيلة الأمنية فيما يتعلق بالإنذار والاستجابة السريعة للسلوكيات الضارة، وما إلى ذلك.

4.7 المبادئ التوجيهية الأمنية لطبقة النفاذ

تركز المبادئ التوجيهية الأمنية لطبقة النفاذ على آلية الاستيقان والسطح البيني لبرمجة التطبيقات (API).

1.4.7 المبادئ التوجيهية الأمنية لآلية الاستيقان

تشمل المبادئ التوجيهية الأمنية لآلية الاستيقان ما يلي:

أ) يوصى بدعم خدمات الاستيقان المعزز، مثل استيقان تسجيل الدخول لمرة وحيدة (SSO) والاستيقان متعدد العوامل وما إلى ذلك.

ب) يوصى بفرض سياسات كلمات مرور قوية، مثل زيادة تعقيد كلمات المرور وتحديث كلمات المرور بانتظام وما إلى ذلك.

ج) يوصى بدعم آلية استيقان على أساس القائمة البيضاء، مثل إعداد قائمة بيضاء بالعناوين IP، وما إلى ذلك.

2.4.7 المبادئ التوجيهية الأمنية للسطح البيني لبرمجة التطبيقات

تشمل المبادئ التوجيهية الأمنية للسطح البيني لبرمجة التطبيقات ما يلي:

أ) يوصى بتمكين المديرين من تخويل النفاذ إلى السطوح البينية لبرمجة التطبيقات، مثل تشكيل الحد الأقصى من المرات التي يمكن للمستعمل النفاذ فيها إلى السطوح البينية لبرمجة التطبيقات، وإجمالي عدد التوصيلات التي يمكن أن تدعمها السطوح البينية لبرمجة التطبيقات وما إلى ذلك.

ب) يوصى بدعم خصائص المراقبة في الوقت الفعلي لتدفقات الشبكة بين العملاء السطوح البينية لبرمجة التطبيقات، وإعداد إنذارات وتمكين الاستجابة للحوادث المتعلقة بحركة الشبكة غير الاعتيادية.

ج) يوصى بالتحقق من صحة مدخلات السطوح البينية لبرمجة التطبيقات للحيلولة دون وقوع الهجمات الأمنية المختلفة.

د) يوصى بدعم نقل البيانات الأساسية عبر قناة مأمونة، على سبيل المثال عبر قناة مجفرة وما إلى ذلك.

هـ) يوصى بفرض الفحص وإزالة الحساسية بشكل ثنائي الاتجاه بين العملاء السطوح البينية لبرمجة التطبيقات قبل نقل البيانات.

و) يوصى بدعم التحقق من سلامة البيانات واكتشاف تلف البيانات أو فقدانها أثناء عمليات النقل.

5.7 المبادئ التوجيهية الأمنية لإدارة الأمن

تشمل المبادئ التوجيهية الأمنية لإدارة الأمن ما يلي:

أ) يوصى باستخدام إدارة الهوية والنفاذ (IAM) وتدقيق التحكم في النفاذ، بما في ذلك سجلات التشغيل والصيانة، وسجلات النفاذ إلى البيانات، وفحص سلوك النفاذ، وإدارة المفاتيح، وتجفير البيانات.

ب) يوصى باستخدام آليات الكشف والحماية المنطقية والفعالة بما في ذلك التكرار الأمني للبنى التحتية، ومسح مواطن الضعف، وأنظمة IPS/IDS، وجدر الحماية، وأجهزة الأمن الافتراضية.

ج) يوصى باستخدام تقنيات التعزيز الأمني لتقليل سطح الهجمات للبنية التحتية والمنصة.

د) يوصى بترقية التصحيحات والإصدارات بانتظام للبنية التحتية للبيانات الضخمة ومنصتها.

بيبليوغرافيا

[b-ITU-T X.800] Recommendation ITU-T X.800 (1991), *Security architecture for Open Systems Interconnection for CCITT applications.*

[b-ITU-T X.810] Recommendation ITU-T X.810 (1995), *Information technology – Open System Interconnection – Security frameworks for open system: Overview.*

[b-ITU-T X.1158] Recommendation ITU-T X.1158 (2014), *Multi-factor authentication mechanisms using a mobile device.*

[b-ITU-T X.1217] Recommendation ITU-T X.1217 (2021), *Guidelines for applying threat intelligence in telecommunication network operation.*

[b-ITU-T X.1245] Recommendation ITU-T X.1245 (2010), *Framework for countering spam in IP-based multimedia applications.*

[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.1524] Recommendation ITU-T X.1524 (2012), *Common weakness enumeration.*

[b-ITU-T X.1631] Recommendation ITU-T X.1631 (2015), *Information technology – Security techniques – Code of practice for information security controls based on ISO/IEC 27002 for cloud services.*

[b-ITU-T Y.2052] Recommendation ITU-T Y.2052 (2008), *Framework of multi-homing in IPv6-based NGN.*

[b-ITU-T Y.2201] Recommendation ITU-T Y.2201 (2009), *Requirements and capabilities for ITU-T NGN.*

[b-ITU-T Y.2244] Recommendation ITU-T Y.2244 (2019), *Service model for a cultivation plan service at the pre-production stage.*

[b-ITU-T Y.3500] Recommendation ITU-T Y.3500 (2014), *Information technology – Cloud computing – Overview and vocabulary.*

[b-ITU-T Y.3502] Recommendation ITU-T Y.3502 (2014), *Information technology – Cloud computing – Reference architecture.*

[b-ISO/IEC 18014-2] ISO/IEC 18014-2:2009, *Information technology – Security techniques – Time-stamping services – Part 2: Mechanisms producing independent tokens.*

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

[b-ISO/IEC 19944] ISO/IEC 19944:2016, *Information technology – Cloud services and devices: Data flow, data categories and data use.*

[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 27000:2016, *Information technology –Security techniques – Information security management systems – Overview and vocabulary.*

[b-ISO/IEC 27729] ISO/IEC 27729:2012, *Information and documentation – International standard name identifier (ISNI).*

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

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