الاتحـــــــــــاد الدولـــــــــــي للاتصـــــــــــالات

ITU-T

قطاع تقييس الاتصالات
في الاتحاد الدولي للاتصالات

X.1751

(2020/09)

السلسلة X: شبكات البيانات والاتصالات بين الأنظمة المفتوحة ومسائل الأمن

أمن البيانات – أمن البيانات الضخمة

المبادئ التوجيهية الأمنية لمشغلي الاتصالات بشأن إدارة دورة حياة البيانات الضخمة

التوصية ITU-T X.1751

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	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.1360
أمن أنظمة النقل الذكية (ITS)	X.1389–X.1370
أمن سجل الحسابات الموزع	X.1429–X.1400
أمن سجل الحسابات الموزع	X.1449–X.1430
البروتوكول الأمني (2)	X.1459–X.1450
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
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**
أمن شبكات الجيل الخامس	X.1819–X.1800

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

التوصية ITU-T X.1751

المبادئ التوجيهية الأمنية لمشغلي الاتصالات بشأن إدارة دورة حياة البيانات الضخمة

ملخص

تحلل التوصية ITU-T X.1751 الثغرات الأمنية وتقدم مبادئ توجيهية أمنية لمشغلي الاتصالات بشأن إدارة دورة حياة البيانات الضخمة.

ومع التطور السريع لتكنولوجيا البيانات الضخمة، زادت قيمة البيانات كثيراً. وتتيح البيانات الضخمة فرصاً جديدة لخدمات الاتصالات. ففيما مضى، كان تخزين البيانات وإدارتها يجري بشكل مستقل في أنظمة خدمة اتصالات مختلفة. ولا مَرَدَّ لاتجاهات تجميع ودمج البيانات مع بناء خدمات البيانات الضخمة. وفي عملية تقارب دمج البيانات، تتدفق البيانات على المنصات وفي عمليات الخدمة. وتواجه البيانات العديد من الثغرات الأمنية في مراحل مختلفة من دورة حياتها.

وتعرِّف التوصية ITU-T X.1751 بخصائص محددة لخدمات البيانات الضخمة للاتصالات وفئات البيانات، وتحلل الثغرات الأمنية لإدارة دورة حياة البيانات الضخمة، وتحدد المبادئ التوجيهية الأمنية لمشغلي الاتصالات.

التسلسل التاريخي

الطبعة	التوصية	تاريخ الموافقة	لجنة الدراسات	معرف الهوية الفريد*
1.0	ITU-T X.1751	2020-09-03	17	11.1002/1000/14267

مصطلحات أساسية

إدارة دورة حياة البيانات، خدمات البيانات الضخمة للاتصالات.

* 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 "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.1751

المبادئ التوجيهية الأمنية لمشغلي الاتصالات بشأن إدارة دورة حياة البيانات الضخمة

1 مجال التطبيق

تصف هذه التوصية الثغرات الأمنية وتضع مبادئ توجيهية لإدارة دورة حياة خدمات البيانات الضخمة للاتصالات. وهذه التوصية:

- تعرِّف بخصائص خدمات البيانات الضخمة للاتصالات وفئات البيانات؛
- تحلل الثغرات الأمنية لإدارة دورة حياة خدمات البيانات الضخمة للاتصالات؛
- تحدد المبادئ التوجيهية الأمنية لإدارة دورة حياة البيانات في خدمات البيانات الضخمة للاتصالات.

عندما يقدم مشغلو الاتصالات خدمات البيانات الضخمة، يتمثل الشرط المسبق في الحصول على موافقة صريحة من المشتركين. وبالإضافة إلى ذلك، يوصى مشغلو الاتصالات بتقديم التدابير اللازمة لحماية البيانات طوال عملية خدمة البيانات الضخمة بأكملها.

وتقع آليات حماية فئات البيانات المختلفة خارج مجال تطبيق هذه التوصية.

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.1641] التوصية ITU-T X.1641 (2016)، *مبادئ توجيهية لأمن بيانات عملاء الخدمات السحابية*.

3 التعاريف

1.3 المصطلحات المعرَّفة في وثائق أخرى

تستخدم هذه التوصية المصطلحات التالية المعرَّفة في وثائق أخرى:

1.1.3 البيانات الضخمة (big data) [b-ITU-T Y.3600]: نموذج للتمكين من جمع وتخزين وإدارة وتحليل وعرض مجموعات البيانات الضخمة جداً ذات الخصائص غير المتجانسة، مع إمكانية تحقيق ذلك في ظل قيود الوقت الفعلي.

2.1.3 البيانات الضخمة كخدمة (big data as a service) (BDaaS) [b-ITU-T Y.3600]: فئة خدمة سحابية تتمثل فيها الإمكانات المقدمة لعميل الخدمة السحابية في القدرة على جمع وتخزين وتحليل وعرض وإدارة البيانات باستعمال البيانات الضخمة.

3.1.3 قابلية الربط (linkability) [b-ISO/IEC 20889]: خاصية لمجموعة بيانات تتيح اقتران (عن طريق الربط) سجل يتعلق بأساس بيانات بسجل يتعلق بنفس أساس البيانات في مجموعة بيانات منفصلة.

4.1.3 استخدام اسم مستعار (pseudonymization) [b-ISO/IEC 29100]: العملية المطبقة على المعلومات المحددة لهوية شخص (PII) التي تبدِّل المعلومات المحددة لهوية باسم مستعار.

5.1.3 سياسة الأمن (security policy) [b-ITU-T X.800]: مجموعة معايير لتوفير خدمات الأمن (انظر أيضاً سياسة الأمن القائمة على الهوية والقائمة على القواعد).

2.3 المصطلحات المعرَّفة في هذه التوصية

تعرّف هذه التوصية المصطلح التالي:

1.2.3 دورة حياة البيانات (data lifecycle): عملية البقاء الكاملة بعد إنشاء البيانات، بما في ذلك جمع البيانات، وإرسال البيانات، وتخزين البيانات، واستخدام البيانات (وهي تغطي تحليل البيانات وعرضها بصرياً)، وتبادل البيانات وإتلاف البيانات.

4 المختصرات والأسماء المختصرة

تستخدم هذه التوصية المختصرات والأسماء المختصرة التالية:

2B لمصلحة أعمال *(to Business)*

2C للمستهلك *(to Consumer)*

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

APP تطبيق *(Application)*

BDaaS البيانات الضخمة كخدمة *(Big Data as a Service)*

BSS/OSS نظام دعم الأعمال ونظام دعم التشغيل *(Business Support System and Operation Support System)*

DB قاعدة بيانات *(Database)*

FTP بروتوكول نقل الملفات *(File Transfer Protocol)*

HDFS نظام الملفات الموزعة Hadoop *(Hadoop Distributed File System)*

IoT إنترنت الأشياء *(Internet of Things)*

IP بروتوكول الإنترنت *(Internet Protocol)*

JDBC توصيلية قاعدة بيانات جافا *(Java Database Connectivity)*

LBS خدمة قائمة على الموقع *(Location-Based Service)*

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

MPP المعالج الموازي الضخم *(Massive Parallel Processor)*

OSS نظام دعم التشغيل *(Operation Support System)*

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

REST نقل الحالة التمثيلية *(Representational State Transfer)*

5 الاصطلاحات

في هذه التوصية:

كلمة "**يجب**" تدل على متطلَّب إلزامي يجب التقيّد به بصرامة، ولا يُسمح بأي انحراف عنه في حال ادعاء الامتثال لهذه التوصية.

كلمة "**يوصى**" تدل على متطلَّب يوصى به لكنه غير إلزامي بالمطلق. وبالتالي لا يتعين توفر هذا المتطلَّب لادعاء الامتثال.

كلمة "**يحظر**" تدل على متطلَّب إلزامي يجب التقيّد به بصرامة ولا يسمح بأي انحراف عنه في حال ادعاء الامتثال لهذه التوصية.

عبارة "**من الجائز**" تدل على متطلَّب اختياري مسموح به دون أن ينطوي على أي توصية به. ولا يرمي هذا المصطلح إلى إلزام تطبيق البائع بتوفير هذا الخيار الذي يمكن أن يوفره مشغل الشبكة/مورد الخدمة اختيارياً. وبالأحرى، فإن البائع يمكنه إدراج هذه الخاصية اختيارياً ويدعى إلى الامتثال لهذه التوصية في نفس الوقت.

6 نظرة عامة

مع التطور السريع لتكنولوجيا البيانات الضخمة، زادت قيمة البيانات كثيراً. وتتيح البيانات الضخمة فرصاً جديدة لمشغلي الاتصالات الذين احتفظوا لفترة طويلة بأنواع مختلفة من موارد البيانات، مثل بيانات المكالمات والموقع، والبيانات الشخصية وبيانات مستهلك الاتصالات المتنقلة وبيانات المطاريف، فيما يسمى أنظمة مستودع البيانات. ومع سرعة نشوء البيانات الضخمة، يواظب مشغلو الاتصالات على الابتكار والاستثمار في تطوير خدمة البيانات الضخمة.

وتشتمل خدمات البيانات الضخمة للاتصالات على كميات من المعلومات بوحدات التيرابايت أو حتى البيتابايت. والبيانات المتولدة ذات أنواع مختلفة، من قبيل بيانات مهيكَلة وشبه مهيكَلة وغير مهيكَلة. وتتضمن المصادر بيانات خاصة، مثل المعلومات المحددة لهوية شخص وبيانات سجل النفاذ. ويمكن للمهاجمين استهداف مثل هذه البيانات.

وسابقاً، فُصلت البيانات في أنظمة خدمة الاتصالات المختلفة وأديرت بشكل مستقل. وبالإضافة إلى ذلك، كان يمكن أن توضع هذه الأنظمة في مواقع مختلفة وأن تديرها دوائر مختلفة. ومع تطور خدمة البيانات الضخمة، يقوم مشغلو الاتصالات بتحطيم الحواجز الإدارية وبجمع البيانات من أنظمة منفصلة مختلفة. ويعزز تقارب البيانات كثيراً من قيمة خدمات البيانات الضخمة.

وفي عملية خدمة البيانات الضخمة، تتدفق البيانات عبر منصة البيانات الضخمة وتمر بمراحل مختلفة من دورة الحياة، وفي كل واحدة منها، تواجه المعلومات تهديدات ومخاطر أمنية مختلفة. فعلى سبيل المثال، يمكن أن يؤدي جمع البيانات بشكل غير سليم إلى الكشف غير الملائم عن البيانات. ويمكن أن يحدث النفاذ غير المجاز في مرحلة تخزين البيانات. ويمكن أن يؤدي استخدام البيانات الحساسة إلى مخاطر تسرب البيانات عند تبادل المعلومات. لذلك، تقتضي الضرورة تحليل الثغرات الأمنية وتحديد المبادئ التوجيهية الأمنية لإدارة دورة حياة خدمات البيانات الضخمة للاتصالات.

وتحلل هذه التوصية المخاطر الأمنية وتحدد المبادئ التوجيهية الأمنية لإدارة دورة حياة البيانات الضخمة للاتصالات.

7 خصائص خدمات البيانات الضخمة للاتصالات وفئات البيانات

1.7 خصائص خدمات البيانات الضخمة للاتصالات

يتخذ المزيد فالمزيد من مشغلي الاتصالات خدمات البيانات الضخمة كتوجه استراتيجي مهم للابتكار والتطوير في شركاتهم. فعلى سبيل المثال، يمكن لمشغلي الاتصالات تطوير خدمات البيانات الضخمة من خلال بناء منصات قادرة على التعامل مع البيانات الضخمة أو تشكيل فرق تشغيل متخصصة بها.

ويمكن لمشغلي الاتصالات جمع مجموعة هائلة من بيانات العملاء المتعلقة بالمستخدم الفردي، مثل ملف تعريف المستخدم وأجهزته واستخداماته ومواقعه. ويمكن لمشغلي الاتصالات استخدام التقنيات التحليلية للبيانات الضخمة للاستفادة من هذه البيانات من أجل تطوير الخدمات المتعلقة بمجموعة واسعة من التطبيقات، مثل البيع بالتجزئة والرعاية الصحية والمدن الذكية. ويمكن لمشغلي الاتصالات استخدام هذه الخدمات لتعزيز مصالح أعمالهم أو تسويقها لمقدمي خدمات يشكلون أطرافاً ثالثة في قطاعات الأعمال الأخرى.

بيد أن اتساع وأنواع البيانات التي يستخدمها مشغلو الاتصالات لخدمات البيانات الضخمة هذه يمكن أن يكشف عن قدر مذهل من التفاصيل عن الأفراد، بما في ذلك المعلومات المحددة لهوية شخص (PII) والبيانات الحساسة، مثل المعتقدات الدينية أو الانتماءات السياسية والأسرار التجارية. وهذا الاعتبار مهم بشكل خاص إذا اختار مشغلو الاتصالات إطلاع أطراف ثالثة على هذه البيانات. لذلك، تقتضي الضرورة أن يتعرف مشغلو الاتصالات على التهديدات في دورة حياة البيانات لخدمات البيانات الضخمة الخاصة بهم وأن يتخذوا إجراءات أمنية لحماية مستخدميهم.

2.7 فئات البيانات

ترد في الفقرة التالية أربع فئات رئيسية لبيانات المستخدم في أيدي مشغلي الاتصالات. وبالإضافة إلى ذلك، يتواصل توسع عمق واتساع البيانات مع تطور إنترنت الأشياء (IoT) وخدماتها. وينتج عن هذا التوسع مخاطر جديدة على ثقة المستخدم وأمنه تجب على مشغلي الاتصالات معالجتها تتعلق بما يلي:

1) البيانات المتولدة من نظام دعم الأعمال ونظام دعم التشغيل (BSS/OSS) لدى مشغل الاتصالات، وهي تتكون من هوية المستخدم وطول المكالمة وهدف الاتصال وفاتورة الاتصال وأنواع الخدمة وحتى نوع المطراف؛

2) البيانات المتولدة من نظام دعم التشغيل لدى مشغل الاتصالات (OSS)، وهي في الأساس بيانات سلوك المستخدم، بما في ذلك البيانات المتولدة عبر خدمة الإنترنت المتنقلة، والدردشة، والألعاب وتصفح الإنترنت؛

3) البيانات المستندة إلى معلومات الخدمة القائمة على موقع (LBS) المستخدم، وهي بخلاف الفئتين 1) و2)، ترتبط ارتباطاً وثيقاً بالموقع الفعلي للمستخدم ويمكن استخدامها في مجالات تسويق الأعمال وتنقل السكان والسلامة العامة والتخطيط الحضري؛

4) بيانات الأعمال (2B) أو المستهلك (2C) المتولدة في سيناريو إنترنت الأشياء وهي تتكون من بيانات ضخمة عن "الأشياء" و"الأشخاص" معاً – وهذه البيانات ذات قيمة كبيرة في مجالات الرعاية الصحية والأجهزة القابلة للارتداء والمنازل الذكية.

وتتضمن البيانات الضخمة عن الأشياء: قراءات تؤخذ من عدادات استهلاك الماء والكهرباء والغاز؛ وبيانات المناخ والتلوث التي تجمعها أجهزة الاستشعار؛ وبيانات تتبع شحنات الأصول.

وتتضمن البيانات الضخمة عن الأشخاص: بيانات عن الصحة والشؤون المالية الشخصية؛ وسجل المشتريات.

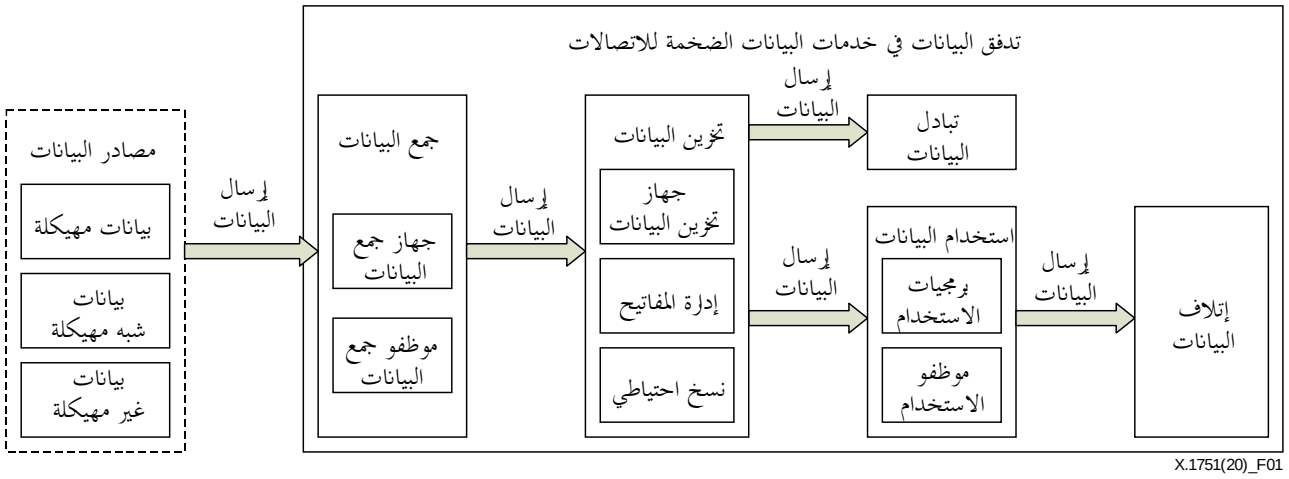
ويجدر بالذكر أن قابلية ربط بعض البيانات يمكن أن تؤدي إلى آثار أكبر على المستخدمين مما هو متوقع، حسب كيفية تصنيف البيانات في البداية؛ فعلى سبيل المثال، فإن بيانات الفئة 4) مغفَلة الهوية التي تحلَل إلى جانب بيانات أخرى قد تجعل هوية الأفراد قابلة للتحديد، مثل المعلومات المحددة لهوية شخص في الفئة 1). لذلك، يوصى بأن تكون قابلية الربط هي الاعتبار الأساسي عند تحديد كيفية تأمين البيانات، حتى في الحالات التي لا يرد فيها تصنيف البيانات فوراً على أنها معلومات محددة لهوية شخص أو غيرها من البيانات الشخصية.

وفي هذه التوصية، يوصى بتأمين البيانات في هذه الفئات الأربع في جميع مراحل دورة حياة البيانات من خلال المبادئ التوجيهية الأمنية.

8 دورة حياة البيانات في خدمات البيانات الضخمة للاتصالات

إن دورة حياة البيانات في خدمات البيانات الضخمة للاتصالات تتكون من ست مراحل أساسية هي: جمع البيانات؛ وإرسال البيانات؛ وتخزين البيانات؛ واستخدام البيانات؛ وتبادل البيانات؛ وإتلاف البيانات. ويمكن أن تتضمن مرحلة إرسال البيانات عدة مراحل.

ويوضح الشكل 1 دورة حياة البيانات في خدمات البيانات الضخمة للاتصالات.



الشكل 1 – دورة حياة البيانات في خدمات البيانات الضخمة للاتصالات

في دورة حياة خدمات البيانات الضخمة للاتصالات، تتمثل البداية في جمع البيانات، والنهاية في إتلاف البيانات. وبعد جمع البيانات، يمكن إرسال البيانات وتخزينها واستخدامها وتبادلها. يمكن أن يحدث إرسال البيانات بين مراحل مختلفة، فبعد جمع البيانات، على سبيل المثال، يمكن إرسال البيانات إلى أجهزة التخزين المتخصصة؛ وأثناء الاستخدام، يمكن إرسال البيانات من أجهزة التخزين إلى برمجيات أو كيان الاستخدام؛ وبعد الاستخدام، تتطلب البيانات منتهية الصلاحية أو عديمة الفائدة الإتلاف.

جمع البيانات: باستخدام أجهزة أو كيانات جمع البيانات المتخصصة، تُجمع أنواع وفئات مختلفة من البيانات في دليل محدد أو دليل مؤقت للتخزين.

إرسال البيانات: تتضمن هذه العملية إرسال البيانات من جهاز جمع البيانات إلى جهاز تخزين ومن التخزين إلى الاستخدام والتبادل. وفي بعض الأحيان تتضمن مرحلة إتلاف البيانات أيضاً إرسال البيانات.

تخزين البيانات: تخزَّن البيانات في أجهزة مخصصة، مثل قواعد البيانات (DB) وأنظمة الملفات الموزعة وصفائف الأقراص. والتجفير والنسخ الاحتياطي للبيانات ضروريان أيضاً للبيانات المهمة.

استخدام البيانات: تَنْفذ برمجيات وتطبيقات تحليل البيانات إلى البيانات وتعالجها لتقدم مجموعة متنوعة من خدمات البيانات الضخمة. ويمكن تبادل البيانات الحساسة الشخصية المتنوعة في هذه العملية.

تبادل البيانات: يُطلِع مقدم خدمة البيانات أو مالك البيانات مقدمين آخرين أو أطراف ثالثة على نتائج معالجة تحليل بياناته أو حتى بيانات المصدر.

إتلاف البيانات: إن البيانات منتهية الصلاحية، خاصة تلك الموجودة في الأجهزة التي تخزن معلومات مهمة أو حساسة، تتطلب الإتلاف الكامل بواسطة آلية أمن مخصصة لهذا الغرض.

9 الثغرات الأمنية في دورة حياة البيانات لخدمات البيانات الضخمة للاتصالات

في عملية خدمات البيانات الضخمة للاتصالات، تتدفق البيانات في كل خطوة من خطوات الخدمة. ويمكن أن تنشأ الثغرات الأمنية من داخل أو خارج العملية. وترتبط الثغرات الأمنية الداخلية بالأجهزة والأنظمة، مثل أجهزة جمع البيانات وأجهزة التخزين وأجهزة الاستخدام. وتحدث الثغرات الأمنية الخارجية بسبب سوء التشكيلة أو سوء الاستخدام. ويمكن الاطلاع على وصف للثغرات المتعلقة بالبيانات في التوصية [b-ITU-T X.1040].

1.9 مرحلة جمع البيانات

1.1.9 ثغرة أمنية في الجهاز والنظام

ثغرات في الجهاز والنظام أو إصابتهما بفيروسات أو برمجيات حصان طروادة، مما يسبب مشاكل أمنية.

2.1.9 ثغرة أمنية في التشكيلة والإدارة

1) إدارة شؤون الموظفين

يمكن تشغيل أجهزة جمع البيانات بشكل غير صحيح أو استخدامها بدون إذن، مما يؤدي إلى مخاطر تسرب البيانات.

2) إدارة الجهاز

يمكن أن تؤدي التشكيلة الضارة أو الخاطئة لأجهزة جمع البيانات إلى جمع بيانات غير مجاز وتسرب البيانات.

وتتراكم البيانات من عدد من أنظمة الأعمال المختلفة الموجودة في مواقع متنوعة وتديرها إدارات مختلفة. يمكن أن تقتحم عقدة خبيثة مجموعة الأجهزة لإجراء عمليات جمع بيانات غير مجازة.

3) إدارة البيانات

يبالَغ في جمع البيانات غير المتعلقة بالغرض المعلَن للاستخدام، وقد يؤدي ذلك إلى تسرب البيانات.

وأثناء مرحلة جمع البيانات، لا يتحكم موظفو جمع البيانات في منطقة تخزين مؤقت للبيانات، مثل مسار عشوائي لمخدم بروتوكول نقل الملفات (FTP)، فتتفاقم مخاطر الكشف عن البيانات أو تغييرها غير المجاز.

2.9 مرحلة إرسال البيانات

1.2.9 ثغرة أمنية في التشكيلة والإدارة

1) إدارة شؤون الموظفين

يقوم المسؤول بتعديل مَنفذ الإرسال أو تشكيلة الإرسال دون إذن، مما يمكن أن يتسبب في تسرب البيانات.

2) إدارة الجهاز

تُرسَل البيانات التي جُمعت عبر قناة غير آمنة، مما يجعل البيانات عرضة للتنصت أو التغيير.

ولم يُستيقَن من سطح بيني للإرسال وبالتالي يحدث توصيل خاطئ أو توصيل ضار.

ولا تحمي آلية الإرسال بين العقد المختلفة كتمان البيانات وسلامتها، مما يؤدي إلى تسرب البيانات ويزيد من خطر التغيير والتنصت والاعتراض.

3) إدارة البيانات

يمكن أن يؤدي غياب حماية الكتمان أثناء إرسال البيانات إلى اعتراض البيانات أو تسرب البيانات.

ويمكن أن يؤدي نقص حماية السلامة أثناء إرسال البيانات إلى التلاعب الخبيث أو إتلاف البيانات.

ويمكن أن يؤدي عدم توفر الحماية أثناء الإرسال إلى اعتراض البيانات أو العبث بها.

3.9 مرحلة تخزين البيانات

1.3.9 ثغرة أمنية في الجهاز والنظام

يؤدي عدم نشر أي برمجيات لمكافحة الفيروسات أو نشر برمجيات أمنية منتهية الصلاحية إلى الكشف عن البيانات الحساسة وتسميمها.

وبرمجيات أمنية مشكَّلة بشكل خاطئ أو غير مصونة تترك البيانات بدون حماية، مما يمكن أن يؤدي إلى الكشف عن البيانات وتسميمها وهجمات مناوئة على مجموعات البيانات.

2.3.9 ثغرة أمنية في التشكيلة والإدارة

1) إدارة شؤون الموظفين

تشكَّل تدابير التحكم في النفاذ بشكل غير صحيح بحيث تتعرض البيانات المخزنة لخطر النفاذ أو التغيير غير المجاز. ويتمكن الأفراد المجاز لهم النفاذ إلى بعض مجموعات البيانات المخزنة من الاستدلال على معلومات تحدد هوية أشخاص أو على بيانات شخصية أخرى لا يجوز لهم النفاذ إليها، بسبب قابلية ربط البيانات.

2) إدارة الجهاز

تتعايش في بيئة تخزين قاعدة بيانات علائقية ونظام الملفات الموزعة Hadoop (HDFS) ومستودع بيانات المعالج الموازي الضخم (MPP). وتؤدي رداءة إدارة الأذونات إلى النفاذ غير المجاز والكشف عن البيانات.

وتخزَّن العديد من البيانات غير المهيكَلة في عُقد مختلفة بشكل منفصل، مما يصعِّب إنفاذ سياسة الأمن نفسها. ويمكن أن تؤدي سياسات أو تعارضات الأمن غير المتسقة إلى نقص الحماية الأمنية وتسرب البيانات.

3) إدارة البيانات

لا تجفَّر البيانات المخزنة، سواء بشكل كامل أو جزئي، مما يزيد من تعرض المستخدمين في حال خرق البيانات المنفعل أو النشط.

تجفَّر البيانات المخزنة؛ غير أن الثغرات المتعلقة بخوارزمية التجفير أو إدارة المفاتيح تزيد من خطر النفاذ غير المجاز إلى البيانات المخزنة أو تغييرها.

ولا تحمى سلامة البيانات حماية نشطة أثناء تخزينها، مما يعرض البيانات إلى تعديل غير مجاز حتى بعد جمعها.

وتتضمن البيانات المخزنة بيانات تجاوزها الزمن أو ليست ذات صلة مباشرة وضرورية للغرض المذكور من الاستخدام. مع زيادة عدد البيانات المخزنة، يزداد تعرض المستخدم في حال حدوث أي اختراق منفعل أو نشط.

ويمكن أن تؤدي آليات النسخ الاحتياطي والاسترداد غير المكتملة للبيانات إلى عدم توفر البيانات.

4.9 مرحلة استخدام البيانات

1.4.9 ثغرة أمنية في الجهاز والنظام

في برمجيات تحليل البيانات الموصولة شبكياً أو القائمة على الحوسبة السحابية توجد ثغرات تعرض البيانات التي تعالجها البرمجيات للخطر.

وتشوب تطبيق العرض البصري لبرمجيات تحليل البيانات إشكالات أمنية يمكن أن يستغلها المهاجمون.

2.4.9 ثغرة أمنية في التشكيلة والإدارة

1) إدارة شؤون الموظفين

في حال نقص في قدرات الاستيقان والإجازة لدى المستخدمين أو تطبيقات العرض البصري، يمكن للمستخدم المزيف أو تطبيق العرض البصري المزيف الحصول على بيانات مرئية، مما يؤدي إلى تسرب بيانات.

2) إدارة الجهاز

يؤدي عدم الاستيقان من هوية أجهزة استخدام البيانات إلى انضمام جهاز غير مجاز إلى منصة البيانات الضخمة. ونتيجة لذلك، تتسرب بيانات أو لا تتيسر لمصلحة أعمال.

3) إدارة البيانات

عند استخدام تطبيقات العرض البصري لبيانات شخصية، بما في ذلك أي معلومات محددة لهوية شخص والبيانات الحساسة، لا تُغفل أو تُحجب هويتها بشكل صحيح فتزداد إمكانية تحديد الهوية.

والبيانات المرئية قابلة للربط إلى حد كبير، مما يزيد من احتمال الاستدلال على الهوية أو البيانات الشخصية الأخرى.

ولا تخزَّن بيانات المخرجات الناتجة عن عمليات تحليل البيانات في بيئة آمنة، أو يُحتفظ ببيانات المخرجات التي تجاوزها الزمن أو انقطعت صلتها المباشرة أو ضرورتها لغرض الاستخدام. وكلما زاد عدد البيانات المحفوظة، ازداد أيضاً تعرض المستخدم في حال حدوث أي اختراق منفعل أو نشط للبيانات.

ولا تخزَّن سجلات البيانات الناتجة خلال هذه المرحلة بشكل آمن، فيمكن استخدامها للاستدلال على البيانات الشخصية في حال خرق البيانات.

5.9 مرحلة تبادل البيانات

1.5.9 ثغرة أمنية في الجهاز والنظام

ثغرات في الجهاز والنظام أو إصابتهما بفيروسات أو برمجيات حصان طروادة، مما يسبب مشاكل أمنية.

2.5.9 ثغرة أمنية في التشكيلة والإدارة

1) إدارة شؤون الموظفين

لم تتحدد بشكل كافٍ المسؤوليات والقدرات الأمنية لمستخدمي البيانات المشتركة، مما يؤدي إلى حماية غير مناسبة للبيانات وتسرب البيانات.

2) إدارة الجهاز

عدم وضوح نطاق وحدود تبادل البيانات؛ وبالإضافة إلى ذلك، نقص في إجراءات المراقبة الأمنية، مما يؤدي إلى تعرض بيانات الشركاء الحساسة بشكل مباشر.

وتفتقر قناة تبادل البيانات إلى الحماية الأمنية، مما يؤدي إلى إفشاء البيانات المهمة أو العبث بها.

3) إدارة البيانات

عدم اكتمال سجلات تسجيل تبادل البيانات، مما يصعِّب تحديد السبب حال وقوع حادث أمني.

6.9 مرحلة إتلاف البيانات

في نهاية هذه المرحلة، إن لم تُتلف البيانات بالكامل، يمكن لموظفين ضارين استرداد البيانات الحساسة، مما يؤدي إلى تسرب بيانات.

7.9 علاقة الثغرة الأمنية بدورة حياة البيانات

تظهر الثغرات الأمنية في مراحل مختلفة من دورة حياة خدمة البيانات الضخمة. ويعرض الجدول 1 نظرة عامة على العلاقة بين الثغرة الأمنية ودورة حياة البيانات في خدمة البيانات الضخمة.

وفي الجدول 1، يشير الحرف "ن" (نعم) في الخلية إلى وجود ثغرة أمنية في تلك المرحلة.

الجدول 1 – العلاقة بين الثغرة الأمنية ومراحل دورة حياة البيانات

الثغرة		مرحلة في دورة حياة البيانات					
		جمع البيانات	إرسال البيانات	تخزين البيانات	استخدام البيانات	تبادل البيانات	إتلاف البيانات
ثغرة الجهاز		ن		ن	ن	ن	
ثغرة في التشكيلة والإدارة	إدارة شؤون الموظفين	ن	ن	ن	ن	ن	
	إدارة الجهاز	ن	ن	ن	ن	ن	
	إدارة البيانات	ن	ن	ن	ن	ن	ن

10 المبادئ التوجيهية الأمنية لدورة حياة البيانات في خدمات البيانات الضخمة للاتصالات

تصف هذه التوصية الآليات التفصيلية المناسبة لجميع فئات البيانات الموضحة في الفقرة 2.7.

1.10 مرحلة جمع البيانات

1.1.10 المبادئ التوجيهية الأمنية للجهاز والنظام

يُتطلب أن تكون البرمجيات الموجودة على الجهاز والنظام المستخدم لجمع البيانات برمجيات محدَّثة ولا تحتوي على ثغرات معروفة.

ويتطلب الجهاز والنظام المستخدم لجمع البيانات تثبيت برمجيات الأمن المتوافقة مع نظام تشغيل الجهاز، مثل برمجيات مكافحة الفيروسات ومكافحة البرمجيات الضارة.

2.1.10 المبادئ التوجيهية الأمنية للتشكيلة والإدارة

1) إدارة شؤون الموظفين

يوصى بإعلام المستخدمين بالبيانات التي تُجمع ولماذا تُجمع، وبالحصول على الموافقة الصريحة من المستخدمين قبل بدء جمع البيانات.

وعند القيام بجمع البيانات، تقتضي الضرورة الاستيقان من موظفي جمع البيانات وتخويلهم.

2) إدارة الجهاز

يوصى بتوصيف آليات الأمن والتدابير المضادة لجمع البيانات، مثلاً للتشدد في الاستيقان من أجهزة جمع البيانات وإجازتها. ويوصى لفئة البيانات أن تلتزم بمبادئ جمع البيانات.

ويُتطلب إعداد خدمة البيانات الضخمة لتحقيق الغرض المقصود من الخدمة. ويُتطلب تحديد البيانات ذات الصلة والضرورية تماماً لجمع البيانات من أجل تحقيق الغرض من الاستخدام.

ويُتطلب توصيف جهاز جمع البيانات وقنوات جمع البيانات وأنساق البيانات وعمليات جمع البيانات وأساليب جمع البيانات.

ويُتطلب إنفاذ الاستيقان، عند النفاذ، من جهاز جمع البيانات ومن موظفي جمع البيانات؛ ويُتطلب توفير وسيلة لكشف سلوك جمع البيانات الشاذ والتحذير منه.

وتتطلب منطقة تخزين البيانات المؤقتة قيوداً صارمة، مثل حظر تصدير البيانات غير المجاز من هذه المناطق إلى موارد التخزين الأخرى، ويوصى بإجازة تعديل منطقة التخزين.

ويوصى بحماية إرسال البيانات التي جُمعت، بما في ذلك البيانات الشرحية، باستخدام خوارزميات التجفير التي تستخدمها وتختبرها أطراف ثالثة موثوقة على نطاق واسع.

وتتعين إدارة وتخزين مفاتيح التجفير بشكل آمن، وحيثما أمكن، إعطاء الأولوية لبروتوكولات التجفير التي تتميز بالسرية المسبقة.

3) إدارة البيانات

يوصى بتحديد التصنيفات المختلفة للبيانات التي جُمعت وفقاً لأهميتها وحساسيتها.

وتُتطلب سجلات التسجيل والتحذير من السلوك الشاذ التالي عند:

- تجاوز جمع البيانات والإرسال المتكررين العتبة المحددة؛
- انقطاع الإرسال أثناء عملية جمع البيانات؛
- تجاوز عتبة سعة التخزين المحددة.

2.10 مرحلة إرسال البيانات

1.2.10 المبادئ التوجيهية الأمنية للتشكيلة والإدارة

1) إدارة شؤون الموظفين

منع المسؤولين من تعديل منفذ الإرسال أو معلمات تشكيلة السطح بيني دُون عِلَّة.

2) إدارة الجهاز

يُتطلب إرسال البيانات عبر قناة مجفرة من طرف إلى طرف.

والسطح البيني للنقل يقدم قدرات الاستيقان لمنع إقامة التوصيلات الخبيثة.

3) إدارة البيانات

يوصى بتنفيذ الكتمان وحماية سلامة البيانات أثناء مرحلة إرسال البيانات.

ويوصى بكشف تلف سلامة البيانات على الفور أثناء الإرسال؛ ويوصى بتنفيذ التدابير اللازمة لاستعادتها بعد اكتشاف الأخطاء.

3.10 مرحلة تخزين البيانات

1.3.10 المبادئ التوجيهية الأمنية للجهاز والنظام

يُتطلب أن تكون البرمجيات الموجودة على الجهاز والنظام المستخدم لجمع البيانات برمجيات محدَّثة ولا تحتوي على ثغرات معروفة.

ويتطلب جهاز التخزين تثبيت برمجيات أمن محدَّثة.

2.3.10 المبادئ التوجيهية الأمنية للتشكيلة والإدارة

1) إدارة شؤون الموظفين

يُتطلب تنفيذ التحكم في النفاذ للمستخدم أو التطبيق، مثل بروتوكول الاستيقان من شبكة بمفتاح سري، وبروتوكول كيربيروس (Kerberos)، والإجازة كثيرة التفاصيل.

ويوصى بدمج عمليات البيانات الهامة في أسلوب التحكم في خزنة التشغيل متعدد الأشخاص، بحيث لا يمكن لشخص واحد أن يمتلك السلطة التشغيلية الكاملة للبيانات المهمة، مثل ما يخصها من مخرجات الدُفعة والنسخ والإتلاف والنشر والاستخدام.

2) إدارة الجهاز

يجب أن تَحصر أساليب الإجازة النفاذ في الأفراد الضروريين لأداء الغرض المعلن للاستخدام الذي تُجمع البيانات من أجلها. ويجب إعداد الأذونات لمنع نفاذ الأفراد إلى بيانات تزيد عما هو ضروري تماماً لأداء واجباتهم المحددة واحتساب احتمال الاستدلال على البيانات الشخصية جراء إمكانية الربط بين أي مجموعات بيانات مخزنة وأذونات منفصلة بين الأفراد.

3) إدارة البيانات

أ) تقليل البيانات إلى الحد الأدنى

يوصى بتقييد تخزين البيانات، بما في ذلك مخرجات العمليات المنفَّذة خلال مرحلة استخدام البيانات، بحيث يُحتفظ بالبيانات ذات الصلة والضرورية للغرض المذكور من الاستخدام.

ويوصى بتعيين فترات الاحتفاظ القصوى الواضحة لجميع البيانات، استناداً إلى الحد الأدنى الممكن من الوقت الذي يجب فيه الاحتفاظ بالبيانات لتحقيق الغرض المحدد من الاستخدام.

ب) تخزين البيانات المجفَّرة

التخزين المجفَّر ضروري لضمان كتمان البيانات الهامة. ويوصى بدعم نموذج تجفير البيانات التراتبي؛ وتُستخدم آليات تخزين أمن مختلفة وفقاً لمستوى سرية البيانات.

ويوصى باستخدام خوارزميات التجفير التي تنشرها وتختبرها أطراف ثالثة موثوقة على نطاق واسع. وتتعين إدارة وتخزين مفاتيح التجفير بشكلٍ آمن، وحيثما أمكن، تفضَّل بروتوكولات التجفير التي تتميز بالسرية المسبقة.

ج) حماية سلامة البيانات

يوصى بتقديم آلية كشف السلامة لتحديد الضرر وفقدان البيانات بسبب تخزين البيانات.

ويوصى باتخاذ التدابير الضرورية لاستعادة سلامة البيانات بعد اكتشاف الأخطاء [ITU-T X.1641].

ويجب الاحتفاظ بسجلات التدقيق التي توثق أي تغيير في البيانات المخزنة. ويجب تخزين السجلات بشكل آمن ويوصى بتسجيل محاولات تعديلها والإبلاغ عنها.

د) النسخ الاحتياطي للبيانات واستردادها

يوصى بتقديم آليات كاملة للنسخ الاحتياطي للبيانات واستردادها من أجل ضمان قابلية استخدام البيانات وسلامتها.

4.10 مرحلة استخدام البيانات

1.4.10 المبادئ التوجيهية الأمنية للجهاز والنظام

يُتطلب أن تكون البرمجيات الموجودة على الجهاز والنظام برمجيات محدَّثة ولا تحتوي على ثغرات معروفة.

ويوصى لجهاز التخزين تثبيت برمجيات أمن محدَّثة.

2.4.10 المبادئ التوجيهية الأمنية للتشكيلة والإدارة

1) إدارة شؤون الموظفين

يوصى بتقديم استيقان موحد كي تستخدمه تطبيقات (استخدام بيانات) مختلفة للنفاذ إلى منصات البيانات الضخمة، بغض النظر عن نوع السطوح البينية التي تستخدمها التطبيقات، من قبيل السطح البيني لبرمجة تطبيقات نقل حالة تمثيل الموارد (REST API)

وتوصيلية قاعدة بيانات جافا (JDBC). ويمكن أن تكون آلية الاستيقان التفصيلية بروتوكول Kerberos أو بروتوكول النفاذ إلى الدليل الخفيف (LDAP) أو غيرها.

ويوصى بتقديم الإجازة كثيرة التفاصيل كي تستخدمها تطبيقات مختلفة للنفاذ إلى منصات البيانات الضخمة، بما في ذلك الأساليب التالية:

أ) الإجازة كثيرة التفاصيل للنفاذ إلى منصات البيانات الضخمة من خلال أسماء المستخدمين وعنوان بروتوكول الإنترنت (IP) وأسماء التطبيقات (APP)؛

ب) الإجازة كثيرة التفاصيل للنفاذ إلى موارد تخزين، مثل: برمجيات مستودعات البيانات؛ وHive؛ وقاعدة البيانات الموزعة غير العلائقية مفتوحة المصدر (Hbase)؛ وHDFS وقواعد البيانات (DB)؛

ج) الإجازة كثيرة التفاصيل من تشغيلات مختلفة لقاعدة البيانات أو نظام الملفات (من قبيل الاختيار (SELECT) والإدراج (INSERT) والإنشاء (CREATE))؛

د) الإجازة كثيرة التفاصيل لأذونات استيراد وتصدير البيانات؛

هـ) الإجازة كثيرة التفاصيل للنفاذ إلى ملف ودليل نظام الملفات الموزعة Hadoop (HDFS).

2) إدارة الجهاز

يوصى بتقديم آليات المراقبة والإنفاذ بشأن الأنشطة الخبيثة في مرحلة استخدام البيانات.

ويوصى بتقديم مسارات التدقيق الأمني لاختبار مدى كفاية استخدام البيانات، ولضمان الامتثال لسياسة الأمن والإجراءات التشغيلية المعمول بها، وللمساعدة في تقييم الضرر والتوصية بأي تغييرات في ضوابط الأمن، وسياسة الأمن وإجراءات استخدام البيانات.

ويوصى بأن تنظر سياسة التدقيق الأمني في ماهية المعلومات عن استخدام البيانات التي يتعين تسجيلها، وفي ظل أي ظروف، وكذلك في التوصيف النحوي والدلالي الذي سيُستخدم في تبادل معلومات التدقيق الأمني.

3) إدارة البيانات

يعد إسناد اسم مستعار للبيانات ضرورياً في مرحلة استخدام البيانات من أجل حماية البيانات الحساسة. وستوحَّد المبادئ التوجيهية التفصيلية لاستخدام أسماء مستعارة للبيانات وسيُنظر فيها في مرحلة تبادل البيانات اللاحقة.

ويوصى بتدقيق استخدام البيانات الحساسة، مع إنشاء سجلات التدقيق على النحو المحدد في [ITU-T X.1641].

5.10 مرحلة تبادل البيانات

1.5.10 المبادئ التوجيهية الأمنية للجهاز والنظام

يُتطلب أن تكون البرمجيات الموجودة على جهاز ونظام المستخدِم برمجيات محدَّثة ولا تحتوي على ثغرات معروفة.

ويوصى لجهاز التخزين تثبيت برمجيات أمن محدَّثة.

2.5.10 المبادئ التوجيهية الأمنية للتشكيلة والإدارة

1) إدارة شؤون الموظفين

يجب إبلاغ المستخدمين عن البيانات، بما في ذلك البيانات الشرحية وأي من البيانات، التي تنتج عن مخرجات العمليات التي نُفذت خلال مرحلة استخدام البيانات، والتي ستطلع أطراف ثالثة عليها ومن هي هذه الأطراف الثالثة. ويجب الحصول على موافقة صريحة من المستخدم قبل تبادل أي بيانات، بما في ذلك بيانات المخرجات.

2) إدارة الجهاز

يوصى بالتحكم في سلوك تصدير البيانات.

وعند تبادل البيانات مع الخدمات الخارجية، يوصى بوضع حدود لاستخدام البيانات لتفادي إعادة بيع البيانات.

ويوصى بالتفاوض بشأن آليات الحماية الأمنية بين أصحاب المصلحة المعنيين (من قبيل المشغلين الذين تُتناقل البيانات بينهم)، وهي تشمل سياسة الأمن بشأن نقل البيانات المشتركة وتخزينها والنفاذ إليها وإتلافها ومخطط النسخ الاحتياطي في حال الكشف عن البيانات المشتركة.

3) إدارة البيانات

ينطوي إسناد أسماء مستعارة للبيانات على عملية إخفاء المعلومات الأصلية المحددة لهوية شخص والبيانات الحساسة بالأحرف أو البيانات. والغرض من ذلك هو حماية المعلومات المحددة لهوية شخص والبيانات الحساسة.

ويمكن تشكيل تطبيقات مختلفة باستخدام خوارزميات مختلفة لاسم مستعار. ويوصى باستخدام اسم مستعار للبيانات من أجل:

أ) دعم إضافة وإزالة خوارزميات الأسماء المستعارة دينامياً؛

ب) دعم الأسماء المستعارة كثيرة التفاصيل، مما يعني تمكين المسؤول من تشكيل اسم مستعار لجدول معين أو أعمدة معينة في قاعدة البيانات؛

ج) استخدام الخوارزميات العمومية، وتجنب الخوارزميات المملوكة من طرف ثالث؛

د) عدم التأثير كثيراً على استمرارية الأعمال وأداء النظام.

6.10 مرحلة إتلاف البيانات

1.6.10 المبادئ التوجيهية الأمنية لإدارة البيانات

يجب محو البيانات والكتابة فوقها في الحالة الصلبة.

وبعد حذف البيانات، يوصى بالتأكد من أن حيز تخزين موارد، من قبيل الملفات والأدلة وسجلات قاعدة البيانات، في النظام قد أخلي بالكامل ولا يمكن استعادته.

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.1040] Recommendation ITU-T X.1040 (2017), *Security reference architecture for lifecycle management of e-commerce business data*.

[b-ITU-T Y.3600] Recommendation ITU-T Y.3600 (2015), *Big data – Cloud computing based requirements and capabilities*.

[b-ISO/IEC 20889] ISO/IEC 20889:2018, *Privacy enhancing data de-identification terminology and classification of techniques*.

[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، 2021