Union internationale des télécommunications

UIT-T

SECTEUR DE LA NORMALISATION
DES TÉLÉCOMMUNICATIONS
DE L'UIT

X.1641

(09/2016)

SÉRIE X: RÉSEAUX DE DONNÉES, COMMUNICATION ENTRE SYSTÈMES OUVERTS ET SÉCURITÉ

Sécurité de l'informatique en nuage – Bonnes pratiques et lignes directrices concernant la sécurité de l'informatique en nuage

Lignes directrices pour la sécurité des données des clients de services en nuage

Recommandation UIT-T X.1641

RECOMMANDATIONS UIT-T DE LA SÉRIE X

RÉSEAUX DE DONNÉES, COMMUNICATION ENTRE SYSTÈMES OUVERTS ET SÉCURITÉ

RÉSEAUX PUBLICS DE DONNÉES	X.1–X.199
INTERCONNEXION DES SYSTÈMES OUVERTS	X.200–X.299
INTERFONCTIONNEMENT DES RÉSEAUX	X.300–X.399
SYSTÈMES DE MESSAGERIE	X.400–X.499
ANNUAIRE	X.500–X.599
RÉSEAUTAGE OSI ET ASPECTS SYSTÈMES	X.600–X.699
GESTION OSI	X.700–X.799
SÉCURITÉ	X.800–X.849
APPLICATIONS OSI	X.850–X.899
TRAITEMENT RÉPARTI OUVERT	X.900–X.999
SÉCURITÉ DE L'INFORMATION ET DES RÉSEAUX	
Aspects généraux de la sécurité	X.1000–X.1029
Sécurité des réseaux	X.1030–X.1049
Gestion de la sécurité	X.1050–X.1069
Télébiométrie	X.1080–X.1099
APPLICATIONS ET SERVICES SÉCURISÉS	
Sécurité en multidiffusion	X.1100–X.1109
Sécurité des réseaux domestiques	X.1110–X.1119
Sécurité des télécommunications mobiles	X.1120–X.1139
Sécurité de la toile	X.1140–X.1149
Protocoles de sécurité	X.1150–X.1159
Sécurité d'homologue à homologue	X.1160–X.1169
Sécurité des identificateurs en réseau	X.1170–X.1179
Sécurité de la télévision par réseau IP	X.1180–X.1199
SÉCURITÉ DU CYBERESPACE	
Cybersécurité	X.1200–X.1229
Lutte contre le pollupostage	X.1230–X.1249
Gestion des identités	X.1250–X.1279
APPLICATIONS ET SERVICES SÉCURISÉS	
Communications d'urgence	X.1300–X.1309
Sécurité des réseaux de capteurs ubiquitaires	X.1310–X.1339
ECHANGE D'INFORMATIONS SUR LA CYBERSÉCURITÉ	
Aperçu général de la cybersécurité	X.1500–X.1519
Echange concernant les vulnérabilités/les états	X.1520–X.1539
Echange concernant les événements/les incidents/l'heuristique	X.1540–X.1549
Echange de politiques	X.1550–X.1559
Heuristique et demande d'informations	X.1560–X.1569
Identification et découverte	X.1570–X.1579
Echange garanti	X.1580–X.1589
SÉCURITÉ DE L'INFORMATIQUE EN NUAGE	
Aperçu de la sécurité de l'informatique en nuage	X.1600–X.1601
Conception de la sécurité de l'informatique en nuage	X.1602–X.1639
Bonnes pratiques et lignes directrices concernant la sécurité de l'informatique en nuage	**X.1640–X.1659**
Mise en oeuvre de la sécurité de l'informatique en nuage	X.1660–X.1679
Sécurité de l'informatique en nuage (autres)	X.1680–X.1699

Pour plus de détails, voir la Liste des Recommandations de l'UIT-T.

Recommandation UIT-T X.1641

Lignes directrices pour la sécurité des données des clients de services en nuage

Résumé

La Recommandation UIT-T X.1641 fournit des lignes directrices génériques concernant la sécurité des données des clients de services en nuage (CSC) dans le contexte de l'informatique en nuage. Elle analyse le cycle de vie de la sécurité des données des clients CSC et propose des exigences de sécurité à chaque étape du cycle de vie des données. En outre, la Recommandation UIT-T X.1641 donne des lignes directrices concernant le moment auquel chaque contrôle devrait être appliqué pour assurer au mieux la sécurité.

Historique

Edition	Recommandation	Approbation	Commission d'études	ID unique*
1.0	ITU-T X.1641	2016-09-07	17	11.1002/1000/12853

Mots clés

Données des clients de services en nuage, contrôles de sécurité des données, cycle de vie de la sécurité des données.

* Pour accéder à la Recommandation, reporter cet URL http://handle.itu.int/ dans votre navigateur Web, suivi de l'identifiant unique, par exemple http://handle.itu.int/11.1002/1000/11830-en.

AVANT-PROPOS

L'Union internationale des télécommunications (UIT) est une institution spécialisée des Nations Unies dans le domaine des télécommunications et des technologies de l'information et de la communication (ICT). Le Secteur de la normalisation des télécommunications (UIT-T) est un organe permanent de l'UIT. Il est chargé de l'étude des questions techniques, d'exploitation et de tarification, et émet à ce sujet des Recommandations en vue de la normalisation des télécommunications à l'échelle mondiale.

L'Assemblée mondiale de normalisation des télécommunications (AMNT), qui se réunit tous les quatre ans, détermine les thèmes d'étude à traiter par les Commissions d'études de l'UIT-T, lesquelles élaborent en retour des Recommandations sur ces thèmes.

L'approbation des Recommandations par les Membres de l'UIT-T s'effectue selon la procédure définie dans la Résolution 1 de l'AMNT.

Dans certains secteurs des technologies de l'information qui correspondent à la sphère de compétence de l'UIT-T, les normes nécessaires se préparent en collaboration avec l'ISO et la CEI.

NOTE

Dans la présente Recommandation, l'expression "Administration" est utilisée pour désigner de façon abrégée aussi bien une administration de télécommunications qu'une exploitation reconnue.

Le respect de cette Recommandation se fait à titre volontaire. Cependant, il se peut que la Recommandation contienne certaines dispositions obligatoires (pour assurer, par exemple, l'interopérabilité et l'applicabilité) et considère que la Recommandation est respectée lorsque toutes ces dispositions sont observées. Le futur d'obligation et les autres moyens d'expression de l'obligation comme le verbe "devoir" ainsi que leurs formes négatives servent à énoncer des prescriptions. L'utilisation de ces formes ne signifie pas qu'il est obligatoire de respecter la Recommandation.

DROITS DE PROPRIÉTÉ INTELLECTUELLE

L'UIT attire l'attention sur la possibilité que l'application ou la mise en œuvre de la présente Recommandation puisse donner lieu à l'utilisation d'un droit de propriété intellectuelle. L'UIT ne prend pas position en ce qui concerne l'existence, la validité ou l'applicabilité des droits de propriété intellectuelle, qu'ils soient revendiqués par un membre de l'UIT ou par une tierce partie étrangère à la procédure d'élaboration des Recommandations.

A la date d'approbation de la présente Recommandation, l'UIT n'avait pas été avisée de l'existence d'une propriété intellectuelle protégée par des brevets à acquérir pour mettre en œuvre la présente Recommandation. Toutefois, comme il ne s'agit peut-être pas de renseignements les plus récents, il est vivement recommandé aux développeurs de consulter la base de données des brevets du TSB sous http://www.itu.int/ITU-T/ipr/.

TABLE DES MATIÈRES

		Page
1	Domaine d'application	1
2	Références	1
3	Définitions	1
3.1	Termes définis ailleurs	1
3.2	Termes définis dans la présente Recommandation	3
4	Abréviations et acronymes	3
5	Conventions	3
6	Aperçu	3
6.1	Données considérées dans la présente Recommandation	3
6.2	Menaces sur la sécurité des données pour les clients de services en nuage	4
6.3	Exigences existantes concernant la sécurité des données	4
6.4	Cycle de vie de la sécurité des données	5
7	Lignes directrices concernant les contrôles de sécurité des données	6
7.1	Contrôles de sécurité à l'étape de création	6
7.2	Contrôles de sécurité à l'étape de transmission	6
7.3	Contrôles de sécurité à l'étape de stockage	6
7.4	Contrôles de sécurité à l'étape d'utilisation	7
7.5	Contrôles de sécurité à l'étape de migration	7
7.6	Contrôles de sécurité à l'étape de destruction	7
7.7	Contrôles de sécurité à l'étape de sauvegarde et de rétablissement	8
Appendice I – Lignes directrices concernant l'utilisation des contrôles de sécurité		9
Bibliographie		10

Recommandation UIT-T X.1641

Lignes directrices pour la sécurité des données des clients de services en nuage

1 Domaine d'application

La présente Recommandation fournit des lignes directrices concernant la sécurité des données des clients de services en nuage (CSC) dans le contexte de l'informatique en nuage, dans les cas où il appartient au fournisseur de services en nuage (CSP) de veiller à ce que les données soient traitées avec un niveau de sécurité adéquat. Il existe en effet d'autres cas où, pour certains services en nuage, la sécurité des données relève de la responsabilité des clients CSC proprement dits et d'autres cas encore où la responsabilité est partagée.

Dans certains cas par exemple, le fournisseur CSP peut être chargé de restreindre l'accès aux données, tandis qu'il appartient au client CSC de déterminer quels utilisateurs de services en nuage (CSU) devraient bénéficier d'un accès, et de définir le comportement des scripts ou applications utilisés par l'utilisateur CSU pour traiter les données.

La présente Recommandation définit les contrôles de sécurité des données des clients CSC qui peuvent être utilisés aux différentes étapes de l'ensemble du cycle de vie des données. Ces contrôles de sécurité peuvent varier en fonction du niveau de sécurité des données des clients CSC. Par conséquent, la présente Recommandation donne des lignes directrices concernant le moment auquel chaque contrôle devrait être appliqué pour assurer au mieux la sécurité.

2 Références

Les Recommandations UIT-T et autres références suivantes contiennent des dispositions qui, par suite de la référence qui y est faite, constituent des dispositions de la présente Recommandation. Au moment de la publication, les éditions indiquées étaient en vigueur. Toutes les Recommandations et autres références étant sujettes à révision, les utilisateurs de la présente Recommandation sont invités à rechercher la possibilité d'appliquer les éditions les plus récentes des Recommandations et autres références énumérées ci-dessous. Une liste des Recommandations UIT-T en vigueur est publiée périodiquement. La référence à un document figurant dans la présente Recommandation ne donne pas à ce document en tant que tel le statut de Recommandation.

[UIT-T X.1601] Recommandation UIT-T X.1601 (2015), *Cadre de sécurité applicable à l'informatique en nuage.*

[UIT-T X.1631] Recommandation UIT-T X.1631 (2015) | ISO/CEI 27017:2015, *Technologies de l'information – Techniques de sécurité – Code de bonne pratique pour les contrôles de sécurité de l'information fondés sur la norme ISO/CEI 27002 pour les services en nuage.*

3 Définitions

3.1 Termes définis ailleurs

La présente Recommandation utilise les termes suivants définis ailleurs:

3.1.1 authentification [b-NIST-SP-800-53]: vérification de l'identité d'un utilisateur, d'un processus ou d'un dispositif, souvent indispensable pour pouvoir accéder aux ressources d'un système d'information.

3.1.2 informatique en nuage [b-UIT-T Y.3500]: modèle permettant d'offrir un accès via le réseau à un ensemble modulable et élastique de ressources physiques ou virtuelles mutualisables, fournies et administrées à la demande et en libre-service.

NOTE – Comme exemples de ressources, on peut citer les serveurs, les systèmes d'exploitation, les réseaux, les logiciels, les applications et les équipements de stockage.

3.1.3 service en nuage [b-UIT-T Y.3500]: une ou plusieurs capacités offertes par l'intermédiaire de l'informatique en nuage demandées à l'aide d'une interface définie.

3.1.4 client d'un service en nuage [b-UIT-T Y.3500]: partie à une relation commerciale aux fins de l'utilisation de **services en nuage**.

NOTE – Une relation commerciale n'implique pas nécessairement des accords financiers.

3.1.5 données d'un client d'un service en nuage [b-UIT-T Y.3500]: classe d'objets de données qui sont sous le contrôle, pour des raisons juridiques ou autres, du client d'un service en nuage et qui ont été introduits dans le service en nuage, ou qui résultent de l'utilisation des capacités du service en nuage par le client du service en nuage ou au nom de celui-ci via l'interface publiée du service en nuage.

NOTE 1 – Comme exemple de contrôles juridiques, on peut citer les droits d'auteur.

NOTE 2 – Il se peut que le service en nuage contienne ou utilise des données qui ne sont pas des données du client du service en nuage, mais qui sont, par exemple, des données mises à disposition par les fournisseurs de services en nuage, ou des données obtenues auprès d'une autre source, ou encore des données accessibles au public. Toutefois, toutes les données de sortie résultant d'opérations effectuées sur ces données par le client du service en nuage au moyen des capacités du service en nuage seront sans doute des données du client du service en nuage, d'après les principes généraux applicables aux droits d'auteur, sauf indication contraire dans des dispositions particulières de l'accord relatif au service en nuage.

3.1.6 données déduites d'un service en nuage [b-UIT-T Y.3500]: classe d'objets de données qui sont sous le contrôle du fournisseur de services en nuage et qui résultent de l'interaction du client du service en nuage avec ledit service.

3.1.7 fournisseur de services en nuage [b-UIT-T Y.3500]: partie qui met à disposition des services en nuage.

3.1.8 utilisateur de services en nuage [b-UIT-T Y.3500]: personne physique, ou entité agissant en son nom, associée à un client de services en nuage qui utilise des services en nuage.

NOTE – Comme exemples de ces entités, on peut citer les dispositifs et applications.

3.1.9 infrastructure en tant que service (IaaS) [b-UIT-T Y.3500]: catégorie de services en nuage pour laquelle le type de capacités de nuage fourni au client de services en nuage correspond à des capacités d'infrastructure.

3.1.10 multilocataires [b-UIT-T Y.3500]: attribution de ressources physiques ou virtuelles selon laquelle plusieurs locataires ainsi que leurs calculs et leurs données sont isolés les uns des autres et inaccessibles entre eux.

3.1.11 plate-forme en tant que service (PaaS) [b-UIT-T Y.3500]: catégorie de services en nuage pour laquelle le type de capacités de nuage fourni au client de services en nuage correspond à des capacités de plate-forme.

3.1.12 partie [b-UIT-T Y.3500]: personne physique ou morale, constituée ou non en société, ou groupe de l'une ou l'autre de ces personnes.

3.1.13 information d'identification personnelle (PII) [b-ISO/CEI 29100]: toute information qui a) peut être utilisée pour identifier la personne à laquelle elle se rapporte, ou b) est ou peut être directement ou indirectement liée à une personne.

3.1.14 titulaire des informations PII [b-ISO/CEI 29100]: personne physique à laquelle les informations d'identification personnelle (PII) se rapportent.

NOTE – Suivant le pays et la législation en matière de protection des données et de respect de la vie privée, on peut aussi employer le terme "sujet des données" comme synonyme du terme "titulaire des informations PII".

3.1.15 logiciel en tant que service (SaaS) [b-UIT-T Y.3500]: catégorie de services en nuage pour laquelle le type de capacités en nuage fourni au client de services en nuage correspond à des capacités d'application.

3.1.16 locataire [b-UIT-T Y.3500]: un ou plusieurs utilisateurs de services en nuage utilisant en partage l'accès à un ensemble de ressources physiques et virtuelles.

3.1.17 menace [b-ISO/CEI 27000]: cause potentielle d'un incident indésirable, susceptible de nuire à un système ou à une organisation.

3.2 Termes définis dans la présente Recommandation

Aucun.

4 Abréviations et acronymes

La présente Recommandation utilise les abréviations et acronymes suivants:

CSC client de services en nuage (*cloud service customer*)

CSP fournisseur de services en nuage (*cloud service provider*)

CSU utilisateur de services en nuages (*cloud service user*)

IaaS infrastructure en tant que service (*infrastructure as a service*)

PaaS plate-forme en tant que service (*platform as a service*)

PII information d'identification personnelle (*personally identifiable information*)

SaaS logiciel en tant que service (*software as a service*)

5 Conventions

Aucune.

6 Aperçu

6.1 Données considérées dans la présente Recommandation

Les données des clients CSC comprennent les données privées des clients stockées sur une plate-forme de nuage et les données connexes liées aux services en nuage pour les clients CSC, par exemple les informations concernant les comptes, la consignation des connexions et le journal des opérations.

La différence entre les termes client CSC (voir le § 3.1.4) et utilisateur CSU (voir le § 3.1.8) est explicitée davantage ci-après.

Le client CSC est la personne ou l'organisation qui établit la relation juridique avec le fournisseur CSP. Le client CSC peut donc être une entreprise, une filiale, une administration ou un particulier.

L'utilisateur CSU est la personne, l'appareil ou l'application qui utilise le service en nuage souscrit. L'utilisateur CSU peut être un fonctionnaire, une application sur un smartphone, un particulier, ou un membre d'un foyer, par exemple un enfant. En règle générale, le client CSC désigne certains utilisateurs CSU pour faire office d'administrateurs et gérer la relation entre le client CSC et le fournisseur CSP. Un utilisateur CSU agit toujours au nom d'un client CSC. La plupart des utilisateurs CSU qui sont des employés n'ont pas ou quasiment pas besoin d'être au courant des activités du fournisseur CSP ou des services souscrits par le client CSC, sauf si le client CSC décide du contraire (par exemple pour les administrateurs et les auditeurs internes).

Un client CSC peut comprendre plusieurs locataires de services en nuage. Un locataire peut comprendre plusieurs utilisateurs CSU.

6.2 Menaces sur la sécurité des données pour les clients de services en nuage

Etant donné que l'environnement des services en nuage a, en règle générale, une architecture multilocataires, la perte ou la fuite de données représente une grave menace pour le client CSC. L'absence de gestion appropriée des informations cryptographiques, comme les clés de chiffrement, les codes d'authentification et le privilège d'accès, pourrait entraîner des préjudices considérables, tels que la perte de données ou une fuite inattendue de données. Par exemple, l'insuffisance des contrôles d'authentification, d'autorisation et de vérification, la mauvaise utilisation des clés de chiffrement ou d'authentification, les défaillances opérationnelles, les problèmes de destruction des données, les questions de juridiction et de politique, la fiabilité des centres de données et le rétablissement après une catastrophe sont reconnus comme étant au nombre des principales sources de ce type de menaces et peuvent être associés aux problèmes.

En ce qui concerne la sécurité des données en mémoire, étant donné que toutes les données des clients CSC sont en réalité stockées dans les équipements des fournisseurs CSP, et que les ressources de stockage sont partagées par différents clients CSC, plusieurs risques sont possibles, notamment:

1) des personnes en interne chez le fournisseur CSP peuvent, grâce à leurs privilèges, obtenir un accès non autorisé à l'origine de la fuite de données des clients CSC;
2) des utilisateurs malveillants ou pirates peuvent aussi obtenir un accès non autorisé à l'origine de la fuite de données des clients CSC;
3) le flux de données transfrontières peut conduire à une fuite de données, en particulier de données sensibles;
4) des pannes logicielles et matérielles, des coupures de courant et des catastrophes naturelles peuvent entraîner une perte de données.

La sécurité des données dépend aussi du processus de transmission. Des données peuvent être volées ou modifiées pendant la transmission, ce qui peut avoir pour conséquence une atteinte à la confidentialité si les données ne sont pas chiffrées correctement. Si les clients CSC n'ont pas adopté un chiffrement adéquat, les fournisseurs CSP devraient vérifier l'intégrité des données et adopter les mesures de chiffrement correspondantes.

Une autre menace est la fuite de données résiduelles. Lorsqu'un client CSC se désabonne d'un service, ses données sont effacées et l'espace mémoire est libéré ou réattribué à d'autres clients CSC. Il appartient au fournisseur CSP de veiller à ce que les données résiduelles d'un client CSC ou d'un locataire ne puissent pas être récupérées par un autre.

6.3 Exigences existantes concernant la sécurité des données

Le cadre de sécurité applicable à l'informatique en nuage spécifié dans [UIT-T X.1601] définit les exigences relatives à la sécurité des données, y compris l'isolation des données, la protection des données et la protection de la confidentialité.

1) Isolation des données

   Dans le contexte de l'informatique en nuage, un locataire ne peut pas accéder à des données appartenant à un autre locataire, même lorsque les données sont cryptées, sauf autorisation explicite. L'isolation des données peut être logique ou physique, selon la granularité d'isolation requise et le modèle de déploiement des logiciels et des matériels d'informatique en nuage utilisés.

   NOTE – Dans le cas de l'informatique en nuage, l'isolation se fait au niveau du locataire. Un client CSC donné peut avoir plusieurs locataires dans le nuage, par exemple pour séparer ses différentes filiales, divisions ou unités organisationnelles.

2) Protection des données

La protection des données garantit que les données du client CSC et les données déduites d'un service en nuage détenues dans un environnement d'informatique en nuage sont protégées comme il se doit, afin que seules les personnes ou entités autorisées par le client CSC (ou conformément à la législation applicable) puissent avoir accès à ces données ou les modifier. Cette protection peut associer plusieurs méthodes: listes de contrôle d'accès, vérification de l'intégrité, correction des erreurs/récupération des données, chiffrement et autres mécanismes appropriés. Lorsqu'un fournisseur CSP assure le chiffrement des mémoires pour les clients CSC, cette fonction peut correspondre à un chiffrement du côté du client (par exemple, dans une application CSP) ou du côté du serveur.

3) Protection de la confidentialité

Les informations privées peuvent être des informations d'identification personnelles (PII) ou des données d'entreprise confidentielles. La collecte, l'utilisation, le transfert, le traitement, le stockage et la destruction d'informations privées peuvent être soumises à la réglementation ou à la législation sur la confidentialité. Cette restriction s'applique à la fois aux fournisseurs CSP et à leurs clients CSC. Par exemple, un client CSC doit pouvoir à tout moment détruire une table de données contenant des informations privées, même si le fournisseur CSP ne connaît pas le contenu de cette table. Les fournisseurs CSP devront peut-être par ailleurs prendre en charge le traitement des informations, par exemple en faisant une recherche dans les données du client CSC sous leur forme transformée ou cryptée.

La protection de la confidentialité concerne également les informations privées qui peuvent être observées dans le cadre des activités du client CSC ou déduites de celles-ci, comme les tendances commerciales, les relations ou les communications avec d'autres parties, et les niveaux et modèles d'activité.

La protection de la confidentialité doit également permettre de garantir que toutes les informations privées (données observées ou déduites) sont utilisées uniquement aux fins convenues entre un client CSC et un fournisseur CSP.

Une évaluation des risques pour les informations privées (appelée "évaluation des risques liés à la confidentialité") peut aider un fournisseur CSP à identifier les risques précis d'atteinte à la confidentialité associés à une opération envisagée. Le fournisseur CSP devrait identifier et mettre en oeuvre des capacités afin de remédier aux risques concernant la confidentialité mis en évidence dans le cadre de l'évaluation des risques et traiter les informations privées.

NOTE – Dans certaines juridictions, les personnes physiques (c'est-à-dire des utilisateurs humains) sont considérées séparément de leurs employeurs à des fins de confidentialité. Dans ce cas, la confidentialité de l'utilisateur CSU sera protégée comme il se doit, de même que celle du client CSC et du locataire.

6.4 Cycle de vie de la sécurité des données

Basé sur la situation réelle du service en nuage, le cycle de vie de la sécurité des données des clients CSC comprend les étapes suivantes:

1) Création: il vaudrait probablement mieux parler de création/mise à jour car il s'agit de créer ou de modifier aussi bien un élément de données/contenu qu'un document ou une base de données. La création consiste à produire un nouveau contenu numérique, ou à modifier/mettre à jour un contenu existant.

2) Transmission: il s'agit du processus de transfert de données d'un endroit à un autre.

3) Stockage: il s'agit de la mise en mémoire des données numériques dans un certain répertoire, qui a lieu généralement presqu'en même temps que la création.

4) Utilisation: les données sont visualisées, traitées, partagées ou utilisées à d'autres fins dans une certaine activité.

5) Migration: il s'agit du processus de transfert de données entre différents types de mémoire, formats ou systèmes informatiques. C'est un aspect essentiel à prendre en considération pour toute mise en place, modernisation ou consolidation d'un système. La migration des données peut avoir lieu pour diverses raisons, par exemple en cas de remplacement ou de modernisation d'un serveur ou d'un équipement de stockage, d'actualisation d'un site web, de maintenance d'un serveur ou de déménagement d'un centre de données.

6) Destruction: les données sont définitivement détruites à l'aide de moyens physiques ou numériques (par exemple par crypto-déchiquetage).

7) Sauvegarde et rétablissement: les utilisateurs peuvent créer des copies de sauvegarde des données et rétablir les données à partir de ces copies.

7 Lignes directrices concernant les contrôles de sécurité des données

Le présent paragraphe fournit des lignes directrices concernant les contrôles de sécurité aux différentes étapes du cycle de vie de la sécurité des données décrites au § 6.4.

7.1 Contrôles de sécurité à l'étape de création

Les lignes directrices concernant les contrôles de sécurité à l'étape de création sont les suivantes:

a) Les fournisseurs CSP devraient définir des catégories de sensibilité des données. Un étiquetage des données par l'utilisateur peut être utile pour faciliter le classement des données.

b) Les données devraient être classées en fonction de leur sensibilité au moment de leur création.

c) Les fournisseurs CSP devraient envisager des mécanismes basés sur les droits numériques de l'entreprise ou un chiffrement pour protéger les données sensibles contre tout accès non autorisé.

7.2 Contrôles de sécurité à l'étape de transmission

Les lignes directrices concernant les contrôles de sécurité à l'étape de transmission sont les suivantes:

a) Les fournisseurs CSP devraient appliquer des méthodes techniques pour garantir la sécurité des données d'authentification.

b) Les fournisseurs CSP devraient aider les utilisateurs à assurer une transmission en toute sécurité des données de gestion et des données d'exploitation critiques.

c) Toute atteinte à l'intégrité des données devrait être détectée rapidement pendant la transmission, et il convient de prendre les mesures nécessaires pour rétablir l'intégrité des données après la détection d'erreurs.

7.3 Contrôles de sécurité à l'étape de stockage

Les lignes directrices concernant les contrôles de sécurité à l'étape de stockage sont les suivantes:

a) Les fournisseurs CSP devraient déterminer les contrôles d'accès que le client CSC peut utiliser pour les données des utilisateurs stockées dans les répertoires, par exemple ceux définis dans [UIT-T X.1631].

b) Les fournisseurs CSP devraient utiliser une technologie de chiffrement ou d'autres mesures de protection pour garantir un stockage en toute confidentialité des données d'authentification.

c) Les fournisseurs CSP devraient aider les utilisateurs à garantir un stockage en toute confidentialité des données de gestion et des données d'exploitation critiques.

d) Les fournisseurs CSP devraient offrir des méthodes efficaces de protection du disque dur ou adopter des mécanismes de stockage par fragments afin d'éviter que des utilisateurs non

autorisés récupèrent des données d'utilisateur valables sur le disque dur, y compris si celui-ci est volé.

e) Toute atteinte à l'intégrité des données en mémoire devrait être détectée rapidement, et il convient de prendre les mesures nécessaires pour rétablir l'intégrité des données après la détection d'erreurs.

f) Il convient d'offrir à l'utilisateur une option de configuration des paramètres de chiffrement tels que les algorithmes, la force et les mécanismes.

g) Les fournisseurs CSP devraient aider les utilisateurs à choisir un mécanisme de chiffrement d'une tierce partie pour chiffrer les données essentielles.

h) Les fournisseurs CSP devraient permettre de chiffrer les données au moyen de clés sécurisées et de stocker et conserver localement ces clés.

i) Les fournisseurs CSP devraient fournir des méthodes efficaces de protection contre le chargement de fichiers image de machine virtuelle afin d'éviter toute mise en œuvre par des utilisateurs non autorisés sur leurs propres ressources informatiques à partir du disque dur, y compris si celui-ci est volé.

7.4 Contrôles de sécurité à l'étape d'utilisation

Les lignes directrices concernant les contrôles de sécurité à l'étape d'utilisation sont les suivantes:

a) Les fournisseurs CSP devraient autoriser et vérifier l'utilisation des données.

b) L'utilisation des données sensibles devrait faire l'objet d'audits, et des journaux d'audit devraient être produits.

c) Les fournisseurs CSP devraient utiliser des mécanismes de surveillance des activités malveillantes et de lutte contre ces activités, dans le cadre de leurs attributions et droits concernant la détection des menaces et le contrôle de l'utilisation des données.

7.5 Contrôles de sécurité à l'étape de migration

Les lignes directrices concernant les contrôles de sécurité à l'étape de migration sont les suivantes:

a) Il convient d'évaluer la connectivité du réseau avant toute migration des données pour garantir la sécurité du processus de migration.

b) Les fournisseurs CSP devraient veiller à ce qu'il n'y ait pas d'atteinte à l'intégrité et à la confidentialité des données pendant une migration.

c) Les fournisseurs CSP devraient veiller à ce que la migration des données n'ait pas d'incidence sur la continuité des services et des applications.

d) Les fournisseurs CSP devraient mener correctement les activités liées à la sauvegarde et au rétablissement des données pendant la migration des données.

e) Les fournisseurs CSP devraient établir un plan de migration, évaluer sa faisabilité et les risques associés, puis adopter en conséquence des mesures de contrôle des risques en vue de la migration des données.

7.6 Contrôles de sécurité à l'étape de destruction

Les lignes directrices concernant les contrôles de sécurité à l'étape de destruction sont les suivantes:

a) Les fournisseurs CSP devraient pouvoir effacer tous les données de clé relatives aux données chiffrées.

b) Les fournisseurs CSP devraient recourir à une destruction physique, par exemple démagnétiser les supports physiques lors de la mise hors service du matériel de stockage.

c) Les fournisseurs CSP devraient utiliser des techniques de récupération des données pour confirmer les processus de destruction.

d) Les fournisseurs CSP devraient pouvoir fournir des moyens permettant d'effacer les données existantes résultant de la migration de données entre différentes plates-formes de nuage, de la résiliation d'un service et d'un contrat, et des catastrophes naturelles.

e) Les fournisseurs CSP devraient fournir des moyens permettant de supprimer toutes les copies des données.

f) Les fournisseurs CSP devraient veiller à ce que l'espace de stockage des informations d'authentification d'un utilisateur – compte d'utilisateur, mot de passe, etc. – ne soit pas libéré ou réattribué à d'autres utilisateurs tant que ces informations ne sont pas complètement effacées.

g) Les fournisseurs CSP devraient veiller à ce que l'espace de stockage des ressources – fichiers, répertoires, données de la base de données, etc. – ne soit pas libéré ou réattribué à d'autres utilisateurs tant que ces ressources ne sont pas complètement effacées.

h) Les fournisseurs CSP devraient fournir des moyens permettant d'empêcher toute récupération des données détruites.

7.7 Contrôles de sécurité à l'étape de sauvegarde et de rétablissement

Les lignes directrices concernant les contrôles de sécurité à l'étape de sauvegarde et de rétablissement sont les suivantes:

a) Les fournisseurs CSP devraient utiliser des mécanismes de récupération du contenu, comme ceux utilisés pour éviter toute perte de données, pour faciliter l'identification et la vérification des données qui nécessitent une sauvegarde.

b) Les fournisseurs CSP devraient prendre en charge un algorithme de chiffrement approprié pour la sauvegarde à long terme des supports de stockage (archivage) et devraient par exemple utiliser de longues clés de chiffrement et planifier le remplacement par un algorithme de chiffrement amélioré.

c) Les fournisseurs CSP devraient offrir des fonctions de sauvegarde et de rétablissement des données au niveau local. Il convient d'effectuer au moins une fois par semaine une sauvegarde complète des données et au moins une fois par jour une sauvegarde incrémentielle.

d) Il convient de mettre en place un centre à distance pour le rétablissement après une catastrophe, et d'intégrer dans ce centre les installations, par exemple les lignes de communication, équipements de réseau et équipements de traitement des données, qui sont nécessaires pour le rétablissement après une catastrophe.

e) Il convient de mettre en place un centre redondant pour le rétablissement après une catastrophe. Ce centre devrait offrir les fonctionnalités équivalentes de base pour la conduite des activités, et mettre en œuvre une synchronisation des données en temps réel via une liaison haut débit. Il pourrait être utilisé simultanément pour la conduite des activités et le fonctionnement des systèmes de gestion tout en maintenant la continuité des activités grâce à un commutateur d'urgence dans les situations de catastrophe.

f) Pour les données qui sont classées comme importantes ou sensibles, les fournisseurs CSP devraient offrir des fonctions de sauvegarde des données à distance ainsi que la possibilité de rétablir les données dans les meilleurs délais. Pour cela, une solution serait de recourir à un réseau avec un centre pour le rétablissement en cas de catastrophe.

Appendice I

Lignes directrices concernant l'utilisation des contrôles de sécurité

(Cet appendice ne fait pas partie intégrante de la présente Recommandation.)

Le Tableau I.1 fournit des exemples d'ensembles de contrôles qui pourraient être utilisés afin de respecter les lignes directrices pour certains exemples de scénarios de données sur la base du classement des données, pour chaque étape du cycle de vie.

Tableau I.1 – Exemples d'ensembles de contrôles

Type	**Cycle de vie des données**						
	Création	**Transmission**	**Stockage**	**Utilisation**	**Migration**	**Destruction**	**Sauvegarde et rétablissement**
IaaS	7.1 a), b), c)	7.2 a), b), c)	7.3 a), b), c), d), e), h), i)	7.4 a), b), c)	7.5 a), b), c), d), e)	7.6 a), b), c), d), e), f), g), h)	7.7 a), c), d), e), f)
PaaS	7.1 a), b), c)	7.2 a), b), c)	7.3 a), b), c), d), e), f), i)	7.4 a), b), c)	7.5 a), b), c), d), e)	7.6 a), b), c), d), e), f), g), h)	7.7 a), b), c), d), e), f)
SaaS	7.1 a), b), c)	7.2 a), b), c)	7.3 a), b), c), d), e),f), g), h), i)	7.4 a), b), c)	7.5 a), b), c), d), e)	7.6 a), b), c), d), e), f), g), h)	7.7 a), b), c), d), e), f)

Bibliographie

[b-UIT-T Y.3500] Recommandation UIT-T Y.3500 (2014) | ISO/CEI 17788:2014, *Technologies de l'information – Informatique en nuage – Présentation générale et vocabulaire*.

[b-ISO/CEI 27000] ISO/CEI 27000:2014, *Technologies de l'information – Techniques de sécurité – Systèmes de management de la sécurité de l'information – Vue d'ensemble et vocabulaire*.

[b-ISO/CEI 29100] ISO/CEI 29100:2011, *Technologies de l'information – Techniques de sécurité – Cadre privé*.

[b-NIST-SP-800-53] NIST Special Publication 800-53 Revision 4 (2015*), Security and privacy controls for Federal information systems and organizations*, Disponible [vu le 10-12-2016] à l'adresse: <http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf>

SÉRIES DES RECOMMANDATIONS UIT-T

Série A	Organisation du travail de l'UIT-T
Série D	Principes de tarification et de comptabilité et questions de politique générale et d'économie relatives aux télécommunications internationales/TIC
Série E	Exploitation générale du réseau, service téléphonique, exploitation des services et facteurs humains
Série F	Services de télécommunication non téléphoniques
Série G	Systèmes et supports de transmission, systèmes et réseaux numériques
Série H	Systèmes audiovisuels et multimédias
Série I	Réseau numérique à intégration de services
Série J	Réseaux câblés et transmission des signaux radiophoniques, télévisuels et autres signaux multimédias
Série K	Protection contre les perturbations
Série L	Environnement et TIC, changement climatique, déchets d'équipements électriques et électroniques, efficacité énergétique; construction, installation et protection des câbles et autres éléments des installations extérieures
Série M	Gestion des télécommunications y compris le RGT et maintenance des réseaux
Série N	Maintenance: circuits internationaux de transmission radiophonique et télévisuelle
Série O	Spécifications des appareils de mesure
Série P	Qualité de transmission téléphonique, installations téléphoniques et réseaux locaux
Série Q	Commutation et signalisation et mesures et tests associés
Série R	Transmission télégraphique
Série S	Equipements terminaux de télégraphie
Série T	Terminaux des services télématiques
Série U	Commutation télégraphique
Série V	Communications de données sur le réseau téléphonique
Série X	**Réseaux de données, communication entre systèmes ouverts et sécurité**
Série Y	Infrastructure mondiale de l'information, protocole Internet, réseaux de prochaine génération, Internet des objets et villes intelligentes
Série Z	Langages et aspects généraux logiciels des systèmes de télécommunication

Imprimé en Suisse
Genève, 2017