Union internationale des télécommunications

UIT-T

SECTEUR DE LA NORMALISATION
DES TÉLÉCOMMUNICATIONS
DE L'UIT

X.1642

(03/2016)

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 relatives à la sécurité opérationnelle de l'informatique en nuage

Recommandation UIT-T X.1642

Union internationale des télécommunications

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.1642

Lignes directrices relatives à la sécurité opérationnelle de l'informatique en nuage

Résumé

La Recommandation UIT-T X.1642 donne des lignes directrices générales sur la sécurité opérationnelle pour l'informatique en nuage du point de vue des fournisseurs de services en nuage (CSP). Elle analyse les exigences de sécurité et les indicateurs pour le fonctionnement de l'informatique en nuage. On y trouve également un ensemble de mesures et d'activités détaillées en matière de sécurité pour l'exploitation et la maintenance courantes de ces services, destinées à aider les fournisseurs CSP à atténuer les risques liés à la sécurité et à résoudre les problèmes de sécurité pour le fonctionnement de l'informatique en nuage.

Historique

Edition	Recommandation	Approbation	Commission d'études	ID unique*
1.0	ITU-T X.1642	2016-03-23	17	11.1002/1000/12616

Mots clés

Clause de sécurité de l'accord de niveau de service (accord SLA), informatique en nuage, sécurité opérationnelle.

* 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/.

© UIT 2017

Tous droits réservés. Aucune partie de cette publication ne peut être reproduite, par quelque procédé que ce soit, sans l'accord écrit préalable de l'UIT.

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	2
4	Abréviations et acronymes	2
5	Conventions	3
6	Vue d'ensemble	3
7	Exigences relatives à la clause de sécurité de l'accord de niveau de service	4
	7.1 Responsabilités en matière de sécurité entre les fournisseurs CSP et les clients CSC	4
	7.2 Prescriptions de la clause de sécurité de l'accord SLA	5
8	Principes directeurs applicables à la sécurité opérationnelle au quotidien	8
	8.1 Gestion des identités et contrôle d'accès	9
	8.2 Chiffrement des données et gestion des clés	11
	8.3 Surveillance de la sécurité du système	12
	8.4 Retour à la normale après une catastrophe	13
	8.5 Gestion de la configuration de la sécurité	14
	8.6 Traitement des événements de sécurité	15
	8.7 Mise à jour des correctifs	17
	8.8 Sécurisation de la gestion de la configuration	19
	8.9 Plans d'intervention en cas d'urgence	20
	8.10 Sauvegarde	22
	8.11 Audit de sécurité interne	23
Bibliographie		26

Recommandation UIT-T X.1642

Lignes directrices relatives à la sécurité opérationnelle de l'informatique en nuage

1 Domaine d'application

La présente Recommandation clarifie les responsabilités en matière de sécurité assumées par les fournisseurs de services en nuage (CSP) et les clients de services en nuage (CSC) et analyse les exigences ainsi que les catégories de mesures de la sécurité opérationnelle pour l'informatique en nuage. Elle définit un ensemble de mesures et d'activités détaillées en matière de sécurité pour l'exploitation et la maintenance courantes des services et des infrastructures d'informatique en nuage du point de vue des fournisseurs CSP, afin de satisfaire les exigences en matière de sécurité opérationnelle pour l'informatique en nuage.

La présente Recommandation aidera les fournisseurs CSP à réduire les risques opérationnels. Elle est principalement destinée aux fournisseurs CSP, par exemple les opérateurs de télécommunication traditionnels et les fournisseurs de services Internet (FAI).

2 Références

Néant.

3 Définitions

3.1 Termes définis ailleurs

La présente Recommandation utilise les termes suivants définis ailleurs:

3.1.1 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.

3.1.2 services 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.

3.1.3 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.

3.1.4 partenaire de services en nuage [b-UIT-T Y.3500]: partie fournissant un appui ou une aide aux activités d'un fournisseur de services en nuage, d'un client de services en nuage ou des deux.

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

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

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

3.1.8 réseau en tant que service (NaaS) [b-UIT-T Y.3500]: catégorie de services en nuage pour laquelle la capacité fournie au client de services en nuage correspond à des capacités de connectivité de transport et à des capacités de réseau connexes.

3.1.9 partie [b-ISO 27729]: personne physique ou morale, constituée ou non en société, ou groupe de l'une ou l'autre de ces personnes.

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

3.1.11 problème de sécurité [b-UIT-T X.1601]: "difficulté" de sécurité autre qu'une menace directe de sécurité découlant de la nature et de l'environnement d'exploitation des services en nuage, y compris les menaces "indirectes".

3.1.12 domaine de sécurité [b-UIT-T X.810]: ensemble d'éléments, politique de sécurité, autorité de sécurité et ensemble d'activités liées à la sécurité dans lesquels l'ensemble des éléments est assujetti à la politique de sécurité pour les activités indiquées et la politique de sécurité est administrée par l'autorité de sécurité pour le domaine de sécurité.

3.1.13 incident de sécurité [b-UIT-T E.409]: tout événement préjudiciable pouvant menacer certains aspects de la sécurité.

3.1.14 accord de niveau de service (accord SLA) [b-ISO/CEI 20000-1]: accord écrit entre le prestataire de service et le client qui définit les services et les objectifs de service.

3.1.15 logiciel en tant que service (SaaS) [b-UIT-T Y.3500]: catégorie de services en nuage pour laquelle le type de capacité 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 (§ 3.2.6) partageant 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.

3.1.18 vulnérabilité [b-NIST-SP-800-30]: faiblesse dans un système d'information, dans les procédures de sécurité système, les contrôles internes ou la mise en oeuvre, qui pourrait être exploitée par une source de menace.

3.2 Termes définis dans la présente Recommandation

Néant.

4 Abréviations et acronymes

La présente Recommandation utilise les abréviations suivantes:

ACL liste de contrôle d'accès (*access control list*)

API interface de programmation d'application (*application programming interface*)

BIA analyse d'impact sur les activités (*business impact analysis*)

CCTV télévision en circuit fermé (*closed circuit TeleVision*)

CPU unité centrale de traitement (*central processing unit*)

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

CSN partenaire de services en nuage (*cloud service partner*)

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

DB base de données (*database*)

DDoS déni de service réparti (*distributed denial of service*)

DLP prévention de la fuite de données (*data leakage prevention*)

DoS déni de service (*denial of service*)

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

IAM Gestion des identités et de l'accès (*identity and access management*)

IdM gestion d'identité (*identity management*)

IDS système de détection des intrusions (*intrusion detection system*)

IP Protocole Internet (*internet protocol*)

IPS système de prévention des intrusions (*intrusion prevention system*)

ISP fournisseur de services Internet (*Internet service provider*)

IT technologies de l'information (*information technology*)

JIT juste à temps (*just in time*)

LDAP protocole simple d'accès à l'annuaire (*lightweight directory access protocol*)

NaaS réseau en tant que service (*network as a service*)

OS système d'exploitation (*operating system*)

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

RPO objectif de point de reprise (*recovery point objective*)

RTO objectifs de durée de reprise (*recovery time objectives*)

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

SLA accord de niveau de service (*service level agreement*)

SMS service de messages courts (*short message service*)

SSO authentification unique (*single sign-on*)

TIC technologies de l'information et de la communication

VDC centre de données virtuel (*virtual data centre*)

VM machine virtuelle (*virtual machine*)

5 Conventions

Néant.

6 Vue d'ensemble

Compte tenu de l'expansion rapide du marché de l'informatique en nuage et de la mise en place de chaînes de valeur industrielles, les questions de sécurité demeurent un enjeu majeur dont on ne saurait négliger l'importance. Les systèmes d'informatique en nuage, du fait de leur complexité accrue et des volumes gigantesques de données privées des utilisateurs qui sont stockées dans le nuage, sont confrontés à des problèmes beaucoup plus nombreux que les systèmes classiques issus des technologies de l'information (IT). Les questions de sécurité et la protection de la vie privée constituent les facteurs les plus importants lorsque les consommateurs sont amenés à évaluer l'utilisation des services d'informatique en nuage.

L'offre de services en nuage va devenir toujours plus abondante, rendant encore plus urgente la nécessité de trouver des méthodes permettant de garantir la fiabilité de ces services. Par conséquent, il est nécessaire d'examiner de manière approfondie la sécurité opérationnelle de l'informatique en nuage, afin de fournir des principes directeurs à l'intention des fournisseurs de services en nuage (fournisseurs CSP). Ces principes directeurs aideront en effet les fournisseurs CSP à limiter les risques en matière de sécurité, afin de se prémunir contre toute utilisation inappropriée et tout modèle

d'entreprise inacceptable, etc., et à améliorer ainsi le niveau de sécurité global de fonctionnement des services d'informatique en nuage.

Du point de vue des fournisseurs CSP, les principaux problèmes liés à la sécurité opérationnelle sont les suivants:

1) Problèmes de maintenance de l'infrastructure de l'informatique en nuage: Lorsque l'informatique en nuage offre aux utilisateurs une infrastructure IT ou une plate-forme ou un logiciel en tant que service, la stabilité, la fiabilité et la fourniture sécurisée des services en nuage sont des conditions essentielles à l'exercice d'activités commerciales. Afin de veiller à ce que le service à la clientèle ne connaisse aucune interruption, il convient de faire en sorte que l'infrastructure du système en nuage fonctionne en toute fiabilité et d'une manière stable et de prendre toutes les précautions nécessaires pour préserver la sécurité et la confidentialité des informations de l'utilisateur. Même en cas de défaillance négligeable, bon nombre de fournisseurs CSP risquent de rencontrer des problèmes comme la cessation d'activité ou la perte de données. Il leur faut donc réfléchir sérieusement à la manière de repérer rapidement les défaillances et de passer automatiquement au système de secours, sans solution de continuité, afin de protéger la disponibilité du service à la clientèle.

2) Problèmes liés au mode de gestion de l'informatique en nuage: L'informatique en nuage, en raison de ces caractéristiques mêmes – qu'il s'agisse de services interrégionaux, de la puissance de calcul phénoménale, du cloisonnement entre gestion et propriété des données – se distingue des autres services informatiques traditionnels. Ces problèmes exigent donc une gestion efficace et une coopération entre les noeuds de branches pour permettre aux fournisseurs CSP de résoudre les problèmes de sécurité. Ceux-ci seront en effet appelés à prendre un certain nombre de mesures techniques, telles que la gestion de la configuration de sécurité, une répartition judicieuse des pouvoirs en matière de gestion, et l'adoption d'un ensemble de règles et de processus de gestion efficaces, pour empêcher les fuites de données de l'utilisateur. Ainsi, les fournisseurs CSP devraient adopter des mesures visant à empêcher les administrateurs internes d'outrepasser leurs pouvoirs, de façon à empêcher toute utilisation abusive des ressources informatiques en nuage par les utilisateurs.

D'une manière générale, pour que la sécurité des applications du nuage fonctionnant sur l'infrastructure en nuage soit complète, les fournisseurs CSP devraient adopter différentes méthodes techniques et différents mécanismes de gestion, non seulement pour assurer la sécurité, la stabilité et la disponibilité de l'infrastructure en nuage, mais aussi pour préserver la continuité des activités et protéger les données de l'utilisateur des services en nuage exploités.

7 Exigences relatives à la clause de sécurité de l'accord de niveau de service

La clause de sécurité de l'accord de niveau de service (SLA) constitue le facteur déterminant qui permet au fournisseur CSP d'obtenir la confiance de l'utilisateur. La relation entre les clients CSC et les fournisseurs CSP, par exemple les responsabilités en matière de sécurité, devrait être clairement décrite dans la clause de sécurité de l'accord SLA. Les fournisseurs CSP devraient axer leurs mesures de sécurité opérationnelle sur le respect des exigences définies dans la clause de sécurité de l'accord SLA.

7.1 Responsabilités en matière de sécurité entre les fournisseurs CSP et les clients CSC

Les responsabilités incombant aux fournisseurs CSP et aux clients CSC devraient être définies, pour ce qui est de la sécurité de l'informatique en nuage, conformément aux diverses capacités de contrôle de l'infrastructure et des ressources de l'informatique en nuage.

Les responsabilités en matière de sécurité sont étroitement liées au mode de service en nuage, étant donné que celui-ci reflète la capacité de contrôle des ressources dans l'environnement du nuage pour les fournisseurs CSP et les clients CSC. Ainsi, par rapport à une plate-forme en tant que service (PaaS)

ou à une infrastructure en tant que service (IaaS), les fournisseurs CSP, dans un logiciel en tant que service (SaaS), devraient assumer un plus grand nombre de responsabilités en matière de sécurité et disposer d'une capacité accrue de contrôle des ressources.

En ce qui concerne le mode de service de l'infrastructure IaaS, les fournisseurs CSP fournissent les services de l'infrastructure, par exemple le centre de données virtuel (VDC), qui comprend les serveurs hébergés, les ressources de stockage ainsi que les outils de réseau et de gestion. Les principales responsabilités en matière de sécurité incombant aux fournisseurs CSP sont la sécurité matérielle, la sécurité du réseau, la sécurité du système sous-jacent et la fiabilité de l'infrastructure du nuage dans son ensemble. Les clients CSC devraient être chargés de toutes les questions de sécurité d'un niveau supérieur à celui de l'infrastructure du nuage qu'ils achètent, par exemple la sécurité du système d'exploitation (OS) invité, le logiciel d'application, etc.

S'agissant du mode de service de la plate-forme PaaS, les fournisseurs CSP offrent un environnement simplifié et réparti pour la conception, les tests et le déploiement des logiciels. Les fournisseurs CSP devraient être responsables de la sécurité de l'interface de programmation des applications (API) de l'environnement des applications, de la sécurité des intergiciels, de la mise à disposition de la plate-forme en nuage, etc., ainsi que de la sécurité de l'infrastructure sous-jacente. Pour leur part, les clients CSC devraient être responsables de la sécurité des services liés aux applications offerts dans l'environnement de la plate-forme en nuage.

Pour ce qui est du mode de service du logiciel Saas, les fournisseurs CSP devraient garantir la sécurité globale depuis la couche infrastructure jusqu'à la couche application et les clients CSC devraient assurer la sécurité de l'information qui s'y rapporte, telle que la sécurité de la gestion des identités (IdM), la vérification de la fuite de mots de passe, etc.

En outre, les clients CSC devraient examiner les questions de sécurité des terminaux qu'ils utilisent pour accéder au nuage.

7.2 Prescriptions de la clause de sécurité de l'accord SLA

7.2.1 Prescriptions générales

La clause de sécurité de l'accord SLA devrait expressément indiquer les conditions de sécurité des services en nuage, ainsi que les fonctions et responsabilités incombant aux fournisseurs CSP et aux clients CSC.

Du point de vue des clients CSC, ceux-ci devraient être à même d'indiquer leurs exigences concernant la clause de sécurité de l'accord SLA. La clause de sécurité de l'accord SLA peut en effet les aider à veiller à ce que leurs fournisseurs CSP bénéficient d'une protection suffisante en ce qui concerne leurs moyens, leurs ressources et leurs services d'information personnalisés lorsque ceux-ci sont à l'arrêt, en service et en mouvement, et à ce que des mécanismes correctifs aient été mis en place pour respecter la réglementation relative à la confidentialité des données associées à leur compétence juridictionnelle.

Du point de vue des fournisseurs CSP, la clause de sécurité de l'accord SLA énonce les prescriptions et les conditions mesurables de la sécurité du service en nuage fourni, qui peut être évaluée, comparée et personnalisée par les clients CSC. Les fournisseurs CSP devraient mettre en place une série de mécanismes techniques et de gestion appropriés pour améliorer la fiabilité et la sécurité des services en nuage et satisfaire aux prescriptions de la clause de sécurité de l'accord SLA, de façon à obtenir à terme la confiance des clients CSC. Les services en nuage peuvent faire l'objet de différents types d'accords SLA, en fonction du contenu des services, de la qualité de service, voire de la région dans laquelle les services sont fournis, mais il n'en demeure pas moins que les conditions minimales énoncées dans la clause de sécurité de l'accord SLA devraient être conformes aux prescriptions juridiques et réglementaires ainsi qu'aux prescriptions des normes publiques correspondantes du secteur.

Les prescriptions particulières énoncées dans la clause de sécurité de l'accord SLA pourraient être négociées par les fournisseurs CSP et les clients CSC sur la base des prescriptions personnalisées des clients CSC et de leur capacité de contrôle des ressources. Pour les fournisseurs CSP, les éléments de la clause de non-responsabilité devraient être clairement énoncés dans un contrat commercial ou une description de produit, afin d'éviter tout différend inutile ou tout risque pour la sécurité et pour faire en sorte que les fournisseurs CSP ne soient pas tenus responsables en cas de force majeure.

7.2.2 Eléments de la clause de sécurité de l'accord SLA

Les clauses de sécurité de l'accord SLA comprennent, sans toutefois que cette liste soit limitative, les éléments ci-après.

7.2.2.1 Continuité des activités

Les fournisseurs CSP devraient assurer une protection suffisante en cas de catastrophe d'origine humaine ou naturelle, afin de garantir la disponibilité du service et la continuité des activités. Les éléments ou les prescriptions détaillés sont énumérés ci-après:

1) Disponibilité du service

   Pourcentage de temps pendant lequel le service peut être utilisé pendant une période donnée. Pour un service en nuage donné, les conditions relatives à la prestation du service ne devraient en général pas être moins strictes que celles afférentes au service traditionnel issu des technologies de l'information et de la communication (TIC).

2) Temps de rétablissement moyen

   Temps nécessaire à la récupération des données perdues ou au rétablissement du service à la suite d'une défaillance ou d'autres catastrophes.

7.2.2.2 Protection de la sécurité des données

Les fournisseurs CSP devraient mettre en place un programme de protection complet, afin de protéger les données et les autres informations confidentielles du client CSC. Les fournisseurs CSP ainsi que les clients CSC devraient se mettre d'accord sur les mécanismes et prescriptions détaillées à prévoir en la matière.

1) Sécurité matérielle du stockage

   Les fournisseurs CSP devraient adopter des mesures visant à garantir la sécurité matérielle du stockage, par exemple présence d'un gardien aux entrées, système de protection incendie, systèmes d'alimentation électrique de secours, etc.

2) Protection du support de stockage de données

   Les fournisseurs CSP devraient mettre en place des mesures de protection telles que le renforcement des dispositifs, la mise à niveau des correctifs, etc., de manière à améliorer la sécurité du support de stockage des données.

3) Chiffrement des données

   Il conviendra de préciser les données qui sont chiffrées dans le processus de stockage ou de transmission et de décrire de manière détaillée les algorithmes de chiffrement.

4) Contrôle de l'accès aux données

   Il conviendra de définir les mesures de contrôle de l'accès aux données de manière à empêcher tout accès illégal.

5) Isolation des données

   Il convient de noter que les données des différents clients CSC sont isolées, tant logiquement que physiquement.

6) Suppression des données

Il s'agit de donner l'assurance que les données sont supprimées. Il convient de garantir que les données seront supprimées à titre permanent avant que les ressources puissent être allouées à d'autres clients CSC.

7) Sauvegarde des données

Il s'agit de définir les conditions relatives à l'objectif de point de reprise (RPO) et à l'objectif de durée de reprise (RTO), à la politique de conservation, aux mesures associant une sauvegarde sur site et une sauvegarde hors site, etc.

8) Audit d'exploitation des données

Les fournisseurs CSP devraient procéder à un audit de l'exploitation des données des clients CSC et être en mesure de repérer un fonctionnement anormal. L'auditeur devrait être certifié et posséder les qualifications nécessaires en matière d'audit.

9) Conformité des données

La collecte, le transfert, la gestion, le stockage et la destruction des données devraient être conformes aux réglementations et législations applicables de la juridiction compétente des clients CSC. De même, l'obligation de conservation des données devrait être conforme à la durée de conservation autorisée en vertu des différentes restrictions juridictionnelles.

7.2.2.3 Intervention en cas d'urgence

Les fournisseurs CSP devraient fournir un service d'appel direct sur ligne réservée et mettre à disposition un service de réclamation pour cause de dérangement, en horaire 5×8 ou 24 heures sur 24, 7 jours sur 7. En outre, les indicateurs de service devraient comprendre le délai d'acceptation de la défaillance, le délai de résolution des problèmes, etc.

7.2.2.4 Mesures de sécurité

Les fournisseurs CSP devraient prévoir des mesures de sécurité appropriées pour l'ensemble de l'infrastructure informatique en nuage.

1) Mesures concernant la virtualisation informatique

Les fournisseurs CSP devraient mettre en place les mesures disponibles pour assurer l'inspection des flux ainsi que des pare-feux virtuels ou d'autres fonctionnalités de sécurité au niveau de la couche hyperviseur, de façon que le comportement des machines intra-virtuelles (VM) soit visible et contrôlé par les administrateurs.

2) Isolation du réseau et du domaine

Les fournisseurs CSP devraient mettre en place des mesures d'isolation du réseau et du domaine, par exemple des politiques en matière de pare-feu et de liste de contrôle d'accès (ACL) au niveau des routeurs et des contrôleurs de domaine afin d'assurer une stricte isolation des différents clients CSC.

3) Accès privilégié

Les fournisseurs CSP devraient mettre en place des mesures, par exemple un accès juste à temps (JIT), pour assurer un accès privilégié.

4) Authentification

Les fournisseurs CSP devraient appliquer des méthodes d'authentification rigoureuses, par exemple l'authentification multifactorielle, l'authentification au moyen d'empreintes digitales, etc., de façon à renforcer la sécurité de l'authentification.

5) Mesures visant à sécuriser le trafic du réseau

Les fournisseurs CSP devraient mettre en oeuvre les mesures disponibles pour contrer les attaques par déni de service (DoS)/par déni de service réparti (DDoS) et faire échec à

l'encombrement du réseau, en déployant des systèmes de détection ou de prévention des intrusions ou en luttant contre les intrusions dans le réseau.

6) Mesures de lutte contre les logiciels malveillants

Les fournisseurs CSP devraient mettre en oeuvre les mesures disponibles pour prévenir les contaminations dues à des logiciels malveillants ou à des virus.

7) Mise à niveau des correctifs

Les fournisseurs CSP devraient procéder à intervalles réguliers à des mises à niveau des correctifs et à des mises à niveau du logiciel de virtualisation, du système d'exploitation et de la base de données (DB), afin de les tenir à jour.

7.2.2.5 Audit de sécurité

Les fournisseurs CSP devraient procéder périodiquement à des audits de sécurité portant sur l'ensemble du système informatique en nuage. Les audits pourront être exécutés par une équipe d'audit interne indépendante ou par des auditeurs tiers (faisant fonction de partenaires des services en nuage (CSN)). Les résultats de l'audit devraient pouvoir être dûment consultés par les clients CSC.

7.2.2.6 Suivi de la sécurité aux fins de l'amélioration de l'accord SLA

Les fournisseurs CSP devraient prévoir un mécanisme permettant de suivre les paramètres quantitatifs des services en vue d'améliorer l'accord SLA.

1) Objets du suivi

Définir les objets du suivi, tels que l'utilisation de l'unité centrale de traitement (CPU), les alertes de sécurité, etc. La condition de déclenchement devrait également être expressément indiquée.

2) Notification d'un événement concernant la sécurité

Il convient de préciser les modalités ainsi que le délai de notification d'un événement concernant la sécurité. Parmi les modalités de notification figurent le courrier électronique, le téléphone, le service de messages courts ou d'autres moyens négociés par les fournisseurs CSP et les clients CSC. On entend par délai de notification le laps de temps moyen entre le moment où l'événement se produit et celui où les clients CSC sont informés.

Les fournisseurs CSP peuvent mettre à la disposition des clients CSC les capacités appropriées, par exemple l'autosurveillance au niveau du service et la supervision automatique des ressources qui leur sont attribuées.

7.2.2.7 Certification de sécurité

Les fournisseurs CSP devraient être chargés de l'acquisition des certifications de sécurité pertinentes et en assurer la mise à jour régulière, afin de répondre aux besoins des clients CSC.

Les ingénieurs et autres membres du personnel des fournisseurs CSP devraient suivre des cours de formation à la sécurité et être qualifiés pour exploiter la plate-forme informatique en nuage.

7.2.2.8 Documentation relative aux activités liées à la sécurité

Les fournisseurs CSP peuvent fournir les documents relatifs à la sécurité qui feront ressortir les efforts déployés pour améliorer la sécurité de leurs services en nuage, par exemple les mesures de sécurité mises en place, les procédures de gestion de la sécurité, etc. Ces documents devraient être facilement accessibles et pouvoir être consultés ou téléchargés depuis leur portail web.

8 Principes directeurs applicables à la sécurité opérationnelle au quotidien

Les fournisseurs CSP devraient mettre en place des mesures et des activités de sécurité à l'intention des administrateurs et des locataires dans leurs activités de sécurité courantes. La clause de sécurité

de l'accord SLA devrait être mise en oeuvre et garantie par des mesures et des activités de sécurité menées à bien par les fournisseurs CSP. Ces mesures et activités de sécurité sont notamment, sans que cette liste soit limitative, les suivantes:

1) **Mesures de sécurité**: Les fournisseurs CSP sont tenus de prendre une série de mesures de sécurité pour fournir les fonctionnalités et installations de base permettant de veiller à la mise en oeuvre de la sécurité opérationnelle de l'informatique en nuage.
   a) La gestion des identités et le contrôle d'accès sont traités au § 8.1.
   b) Le chiffrement des données et la gestion des clés sont traités au § 8.2.
   c) La surveillance de la sécurité du système est traitée au § 8.3.
   d) La reprise d'activité après une catastrophe est traitée au § 8.4.
   e) La gestion de la configuration de la sécurité est traitée au § 8.5.
2) **Activités relatives à la sécurité**: Les fournisseurs CSP sont tenus de mener des activités périodiques en matière de sécurité afin de régler les problèmes de sécurité, en sécurisant le fonctionnement de l'informatique en nuage.
   a) Le traitement des événements concernant la sécurité fait l'objet du § 8.6.
   b) La mise à niveau des correctifs est traitée au § 8.7.
   c) La sécurisation de la gestion de la configuration est traitée au § 8.8.
   d) L'intervention en cas d'urgence est traitée au § 8.9.
   e) La sauvegarde est traitée au § 8.10.
   f) L'audit de sécurité interne est traité au § 8.11.

8.1 Gestion des identités et contrôle d'accès

8.1.1 Gestion des identités

Les fournisseurs CSP devraient assurer une gestion unifiée des identités à l'intention des administrateurs internes et des locataires externes, qui pourront fournir les données brutes aux fins du contrôle d'accès, de l'autorisation et de l'audit unifiés.

1) La gestion des identités devrait prendre en charge la fédération des identités, qui permettra le partage et la synchronisation des informations concernant les comptes entre différentes applications en nuage dans la même zone de confiance.
2) Elle devrait prendre en charge la gestion des identités pendant leur cycle de vie, qui comprend le contrôle des identités tout au long de leur cycle de vie, par exemple le registre des identités, l'attribution de rôles et de privilèges, la modification de privilèges, la suppression d'identités, etc. De plus, l'enregistrement et la modification des identités devraient faire l'objet de la procédure d'approbation par les administrateurs.
3) Les politiques de gestion des identités comprennent la politique de nommage des comptes concernant des identités, la politique de demande de comptes concernant les identités, etc. Ces ensembles de politiques de sécurité devraient prévoir les dispositions suivantes:
   - Le nom du compte concernant l'identité devrait être unique dans la même zone de confiance.
   - Le compte concernant l'identité devrait être bloqué lorsque des mots de passe non valables sont insérés en permanence.
   - Le compte concernant l'identité devrait être désactivé lorsqu'il reste inutilisé pendant une longue période.
   - Le compte concernant l'identité devrait être interdit en cas de tentatives répétées de connexion pendant une très courte période.

4) Dans le cadre de la gestion unifiée des comptes d'utilisateur, le compte devrait être exact de façon à être associé à des individus particuliers ou à un locataire. Les utilisateurs devraient être identifiés par le compte principal et chaque utilisateur (administrateur ou locataire) devrait avoir uniquement un compte principal. Le compte principal peut créer un sous-compte, lequel peut disposer des privilèges autorisés pour gérer les cellules du réseau, les serveurs de bases de données, les serveurs d'application, etc.

5) L'audit unifié des comptes devrait principalement consister à assigner des comptes d'identité et porter sur le comportement de la connexion et de la déconnexion en fonction des modules de contrôle d'accès, ce qui permettra de repérer les comptes illégaux et les comptes en souffrance, de déceler le compte faisant l'objet d'une autorisation excessive ou d'une absence d'autorisation et d'empêcher les tentatives de connexion à l'aide de comptes abandonnés ou falsifiés. L'audit unifié des comptes devrait soumettre les événements affectant la sécurité des comptes au module ou aux systèmes d'audit de sécurité, afin d'accomplir des fonctions d'audit plus diverses, telles que la détection des intrusions, l'audit de surveillance des pannes, etc.

6) La gestion des identités devrait prendre en charge la gestion des mots de passe de l'utilisateur, qui comprend les ensembles unifiés de politiques relatives au mot de passe de l'utilisateur, sur la base de la politique de sécurité de la plate-forme en nuage, par exemple les algorithmes cryptographiques, la longueur d'un mot de passe, la complexité d'un mot de passe et le cycle de mise à jour d'un mot de passe. Elle devrait également prendre en charge différent types de mots de passe, tels que les mots de passe graphiques, les mots de passe fondés sur le son, etc. En outre, elle devrait prendre en charge les fonctions de synchronisation et de réinitialisation des mots de passe.

7) La gestion des identités devrait offrir une possibilité de libre-service aux locataires dans la gestion des comptes. Certaines tâches de gestion peuvent être effectuées par les locataires eux-mêmes, telles que la modification de certaines propriétés simples de l'utilisateur et la mise à jour des mots de passe, de façon à alléger la charge de travail des gestionnaires en matière de maintenance.

8.1.2 Gestion du contrôle d'accès

Les fournisseurs CSP devraient mettre en place un système unifié et centralisé d'authentification et d'autorisation pour améliorer la sécurité du contrôle d'accès dans les activités courantes. Les journaux opérationnels pour le contrôle d'accès aux systèmes informatiques en nuage devraient être enregistrés à des fins d'audit ultérieur.

1) L'authentification unifiée devrait assurer les fonctions suivantes:

- Prise en charge de l'authentification unique (SSO): cette fonction devrait prendre en charge le réglage des paramètres de l'authentification SSO, tels que la durée de session maximale, le temps de repos maximal et la durée d'existence maximale de la mémoire cache.
- Prise en charge des technologies d'authentification courantes, telles que l'authentification LDAP, l'authentification par certification numérique, l'authentification par jeton, l'authentification biométrique, l'authentification multifactorielle, etc.
- Fourniture de journaux d'authentification détaillés. Cette fonction comprend les identifications de systèmes, la journalisation des utilisateurs, le délai de connexion, le délai de déconnexion, l'adresse IP de connexion, le terminal de connexion, les enregistrements des résultats de la journalisation (succès ou échec).
- Fourniture de méthodes d'authentification différenciées et facultatives, en fonction des différents systèmes et services, de façon à assurer un équilibre entre le niveau de sécurité et la facilité d'utilisation, voire les coûts.

2) L'autorisation unifiée devrait assurer les fonctions suivantes:

- Fourniture d'une autorisation d'accès aux ressources en nuage, en fonction de la définition au préalable des utilisateurs, des groupes d'utilisateurs et du niveau de privilèges des utilisateurs.
- Prise en charge des mécanismes d'autorisation centralisée et d'autorisation hiérarchique; le niveau d'autorisation des administrateurs hiérarchiques autorisés devrait être limité par l'administrateur de l'autorisation.
- Prise en charge d'une politique d'autorisation à granularité fine et d'une politique d'autorisation à granularité grossière.
- Fourniture de journaux d'autorisation détaillés, comprenant les adresses IP, l'opérateur, la durée d'autorisation ainsi que les permissions accordées et supprimées.

3) Autres prescriptions:

- Contrôle d'accès aux journaux. Les fournisseurs CSP devraient veiller à ce que, lorsque des administrateurs peuvent accéder aux journaux, des privilèges aient été accordés à cet effet. Les locataires devraient disposer des privilèges accordés par les administrateurs pour visualiser les journaux qui les concernent, en passant par un site web en libre-service ou par d'autres outils clients.
- Mécanismes de chiffrement: Les données sensibles telles que les données d'authentification et les données d'autorisation, etc., devraient être chiffrées lors de la procédure de stockage et de transmission.
- Tous les journaux opérationnels relatifs aux clients CSC devraient être visibles.

8.2 Chiffrement des données et gestion des clés

Le chiffrement et la gestion des clés constituent les principaux mécanismes permettant de protéger les données dans les systèmes informatiques en nuage. Le chiffrement offre un moyen de protection des ressources, tandis que la gestion des clés permet de contrôler les clés de chiffrement qui sont utilisées pour protéger les ressources.

Il convient de définir clairement la mise en oeuvre concrète du chiffrement dans la clause de sécurité de l'accord SLA. En outre, le chiffrement devrait être conforme aux normes pertinentes du secteur et du gouvernement. Les fournisseurs CSP ou les clients CSC devraient tenir dûment compte des éléments suivants:

1) Chiffrement de la transmission des données dans le réseau. Il est tout particulièrement important de sécuriser les justificatifs d'identité tels que les informations financières, les mots de passe, etc.

2) Chiffrement des données statiques sur le disque ou dans la base de données. Ce mécanisme pourrait être utilisé pour faire échec aux fournisseurs CSP malveillants ou aux locataires malveillants situés au voisinage.

3) Chiffrement des données dans les supports de sauvegarde. Ce mécanisme pourrait être utilisé pour empêcher la fuite de données lorsque des supports de sauvegarde ont été perdus ou volés.

Si le fournisseur CSP est le principal responsable du chiffrement des données, la gestion des clés constitue une question essentielle dans les opérations courantes. Le fournisseur CSP devrait définir et exécuter une gestion des clés intégrée tout au long des différentes étapes, notamment pendant la création, l'utilisation, le stockage, la sauvegarde, le rétablissement, la mise à jour et la destruction. Les fournisseurs CSP devraient également tenir compte des questions suivantes:

1) Protection du stockage des clés: Le stockage des clés doit être protégé comme tout autre donnée sensible et son niveau de sécurité doit même être plus élevé que les autres. Seule une entité spéciale peut accéder au stockage des clés. il est également nécessaire de concevoir des

politiques connexes, par exemple la séparation des rôles pour assurer un contrôle d'accès plus strict.

2) Sauvegarde et rétablissement: Etant donné que la perte imprévue d'une clé particulière risque de détruire un service, il est nécessaire de mettre en place une solution de sauvegarde et de rétablissement des clés.

3) Introduction de la tierce partie pour la gestion des clés: Grâce à diverses mesures de séparation des tâches, ce mécanisme pourrait aider les fournisseurs CSP à éviter toute incompatibilité avec les prescriptions juridiques lorsque des données figurant dans les systèmes informatiques en nuage sont déclarées comme étant fournies.

8.3 Surveillance de la sécurité du système

Au cours des opérations courantes, les fournisseurs CSP devraient procéder à une surveillance centralisée de la sécurité en temps réel dans la plate-forme et l'infrastructure en nuage, qui comprend l'état de fonctionnement de diverses ressources physiques et virtuelles. En examinant les principales dispositions de l'accord SLA (par exemple la qualité de fonctionnement du réseau, l'utilisation des ressources du serveur et du stockage, etc.), et en analysant tous les types de journaux, les fournisseurs CSP peuvent procéder à la gestion des défaillances, à la gestion de la qualité de fonctionnement et à la gestion automatique de l'inspection pour atteindre l'objectif d'une surveillance en temps réel ou quasi réel de l'état de fonctionnement des ressources en nuage.

En général, les journaux de surveillance sont gérés et rigoureusement protégés par les fournisseurs CSP. Cependant, dès que les clients CSC en ont besoin, les fournisseurs CSP pourraient leur fournir les journaux de surveillance connexes dont ils ont besoin. Ainsi, les clients CSC auront peut-être besoin des journaux de surveillance connexes pour résoudre des problèmes en cas d'urgence.

Les fournisseurs CSP peuvent également déceler par anticipation des risques opérationnels potentiels et les résoudre en temps voulu. En outre, les fournisseurs CSP devraient offrir une possibilité d'analyse de corrélation entre les clients CSC et les services fournis par les fournisseurs CSP, qui pourra être utilisée pour établir un diagnostic du niveau de qualité et de l'état de la sécurité des services en nuage.

Il existe deux types de modes de surveillance de la sécurité: la surveillance automatique et l'inspection manuelle, qui s'appuient sur les moyens techniques et la gestion des différents fournisseurs CSP. Les objectifs de la surveillance de la sécurité sont les suivants:

1) Surveillance de l'état de fonctionnement de l'infrastructure informatique en nuage: Les fournisseurs CSP devraient offrir la capacité de recueillir et de surveiller les journaux d'événements de sécurité, les informations de vulnérabilité, l'altération de la configuration du dispositif de sécurité, l'état de la qualité de fonctionnement et l'état opérationnel de tous les objets de l'infrastructure informatique en nuage, qui comprennent les ressources de la machine virtuelle (VM), la plate-forme de gestion de l'informatique en nuage, les dispositifs de sécurité, la base de données, etc. Cette surveillance permettra de mieux sensibiliser les fournisseurs CSP à l'état de fonctionnement général et à l'état opérationnel de l'infrastructure en nuage.

2) Détection d'un comportement anormal: On entend par comportement anormal une connexion illégale, l'accès illégal à la plate-forme de gestion du nuage et l'accès en violation à d'autres ressources, les modifications anormales apportées aux configurations de l'équipement du réseau et des machines virtuelles, ou d'autres attaques par pénétration, qui peuvent être mises en oeuvre à l'aide de moyens techniques, tels que les outils d'audit intégrés, les logiciels DLP ou d'autres outils de sécurité.

3) Surveillance d'un trafic anormal dans le réseau: Les fournisseurs CSP devraient être dotés des moyens leur permettant de déceler et d'analyser un trafic anormal dans le réseau physique et virtuel, en particulier le trafic intra-machines virtuelles. Il est nécessaire de se tenir informé

du trafic de réseau et de l'état de la qualité de fonctionnement, pour aider les fournisseurs CSP à améliorer leur capacité de se prémunir contre les attaques par des vers, les attaques en cas de trafic anormal et les autres menaces potentielles dans l'environnement de l'informatique en nuage.

4) Surveillance de la sécurité physique: La surveillance de la sécurité physique comprend le système de contrôle de la température et l'humidité, la télévision en circuit fermé (CCTV), la présence d'un gardien aux entrées, le système de protection incendie, les climatiseurs, le système d'alimentation, les grillages de protection, etc., qui peuvent faire l'objet d'inspections journalières.

Enfin et surtout, les fournisseurs CSP devraient procéder à une vérification complète de l'environnement de l'informatique en nuage pour connaître l'état de fonctionnement des services informatiques en nuage lors des activités courantes et de la maintenance périodique. Les fournisseurs CSP pourront ainsi déceler différentes indications, telles que la qualité de fonctionnement du réseau, la qualité de fonctionnement des machines virtuelles et la qualité de service orientée vers les clients CSC, etc. En outre, le processus de vérification pourra être personnalisé de manière à prendre en charge les alertes de seuil, voire les alertes de valeurs de référence. A partir des renseignements de surveillance obtenus, les fournisseurs CSP devraient être à même de mettre en évidence rapidement les problèmes existants dans le réseau, le stockage, les machines physiques et les plates-formes virtuelles en cas de défaillance.

Les fournisseurs CSP devraient en outre se doter des moyens nécessaires pour localiser les autres clients CSC susceptibles d'être affectés au moyen d'une analyse de corrélation pour chaque défaillance particulière en partant de l'hypothèse selon laquelle les clients CSC sont confrontés aux mêmes insuffisances et ont les mêmes applications ainsi que la même version spécifique de système OS, etc.

8.4 Retour à la normale après une catastrophe

Les fournisseurs CSP devraient appliquer des mesures de sécurité en vue du rétablissement après une catastrophe, en offrant le même niveau de sécurité que les systèmes d'origine. Parmi les techniques utilisées dans le cadre des mesures de sécurité figurent les grappes de serveurs, la duplication miroir synchrone à distance et la duplication miroir asynchrone à distance, qui visent à offrir une capacité de secours automatique pour le retour à la normale après une catastrophe.

1) Grappes de serveurs

Les grappes de serveurs permettent de coordonner et de gérer les erreurs et les défaillances des différentes composantes et d'ajouter des composantes aux grappes de manière transparente, avec l'élasticité et la modularité nécessaires pour assurer une qualité de fonctionnement suffisante.

2) Duplication miroir synchrone à distance

Grâce au logiciel de duplication miroir à distance, les données du site primaire sont reproduites de manière synchrone et transmises vers un site distant. Une fois que le site primaire connaît une défaillance, les programmes en cours basculeront sur le site distant. La duplication miroir synchrone à distance permet de garantir la poursuite des activités sans perte de données. Le coût de cette méthode est cependant élevé, étant donné qu'elle dépend d'un logiciel de duplication miroir spécialement conçu à cet effet et d'une largeur de bande suffisante du réseau. La duplication miroir synchrone à distance est régulièrement mise en oeuvre dans les systèmes présentant un niveau de sécurité élevé.

3) Duplication miroir asynchrone à distance

Il s'agit d'une autre méthode de duplication miroir à distance dont le coût est généralement inférieur à celui de la duplication miroir synchrone à distance. Les données du site primaire sont périodiquement reproduites et transmises vers un site distant. Si la procédure se déroule

de manière satisfaisante, elle permet de garantir qu'il existe une copie complète dans le site distant, sans dégradation de la qualité de fonctionnement du site primaire. Toutefois, en cas de problème pendant la période de duplication miroir, la perte de données est inévitable. On pourra opter pour la duplication miroir asynchrone à distance après une évaluation suffisante des risques.

8.5 Gestion de la configuration de la sécurité

La configuration de la sécurité englobe les règles de sécurité configurées dans la plate-forme du nuage, le réseau, les machines virtuelles et diverses composantes d'application. Elle diffère d'une politique de sécurité de haut niveau, qui fixe l'approche suivie par l'organisation pour atteindre ses objectifs en matière de sécurité de l'information.

Les fournisseurs CSP devraient exécuter la gestion intégrée de la configuration de la sécurité, afin d'assurer une mise en oeuvre efficace et un déploiement rapide de la configuration de la sécurité.

Lors de la gestion de la configuration de la sécurité, il est suggéré que les fournisseurs CSP définissent des modèles de configuration de la politique de sécurité ainsi que des bases de référence de la politique de configuration de la sécurité. De plus, les fournisseurs CSP devraient adopter des mesures visant à garantir l'homogénéité et l'efficacité de la configuration de la sécurité lorsque l'environnement du nuage évolue, et à isoler la configuration de la sécurité entre clients CSC dans un environnement multilocataires.

Les modèles de configuration de la sécurité comprennent les principaux modèles de configuration de la sécurité dont l'environnement de l'informatique en nuage actuel a besoin, tels que la gestion des comptes, l'authentification, les politiques de contrôle d'accès, les politiques en matière d'audit, les politiques de réponse dynamique, les politiques de mise à jour des applications et des logiciels, les politiques en matière de sauvegarde et de rétablissement, etc.

Les bases de référence de la configuration de la sécurité offrent un critère permettant de répondre aux impératifs de configuration de la sécurité de l'environnement de l'informatique en nuage dans son intégralité, ce qui peut aider les fournisseurs CSP à déterminer si la configuration actuelle de la sécurité satisfait ou non le niveau de sécurité fondamental, et fournit par ailleurs des directives détaillées pour le renforcement. Les catégories de bases de référence de la configuration de la sécurité devraient comprendre, sans toutefois que cette liste soit limitative, les éléments suivants: bases de référence de la configuration de la sécurité du système d'exploitation, des bases de données, des pare-feux, de la commutation, des routeurs, etc.

La gestion de la configuration de la sécurité fait intervenir les mesures suivantes:

1) Gestion du modèle de configuration de la sécurité

   Les fournisseurs CSP devraient définir les principaux modèles de sécurité en fonction des exigences de l'environnement du nuage, afin d'accélérer et de faciliter le déploiement de la configuration de la sécurité. La gestion du modèle de configuration de la sécurité devrait prendre en charge des modèles personnalisés et mettre à jour et optimiser en permanence les modèles en fonction de l'évolution de la plate-forme du nuage, de l'état du réseau, des impératifs de service, etc.

   De plus, les fournisseurs CSP devraient offrir aux clients CSC la possibilité de personnaliser de nouveaux modèles de configuration de la sécurité en fonction de leurs propres besoins. En outre, les clients CSC devraient être responsables de l'efficacité de la configuration de la sécurité qu'ils ont personnalisée.

2) Gestion du processus de configuration de la sécurité

   Les fournisseurs CSP devraient démontrer l'efficacité de la configuration de la sécurité. La configuration de la sécurité peut être configurée en fonction des besoins des clients CSC et des services en nuage. Le principal processus de gestion de la configuration de la sécurité

comprend la demande de configuration, l'approbation de la configuration, les tests et la validation technique de la configuration, la mise en oeuvre, l'archivage de la configuration et le rapport sur les résultats.

3) Gestion des bases de référence de la configuration de la sécurité

Les fournisseurs CSP devraient concevoir les bases de référence de la configuration de sécurité en examinant de manière détaillée les impératifs de sécurité de la plate-forme informatique en nuage, du service en nuage, des clients CSC, de la clause de sécurité de l'accord SLA, etc.

Le processus principal de gestion des bases de référence de la configuration de la sécurité comprend la demande et l'enregistrement de la vérification de la configuration de la sécurité, l'approbation, la mise en oeuvre de la vérification, le rapport sur les résultats de la vérification, la mise en oeuvre du renforcement et le rapport sur les résultats du renforcement. La vérification de la configuration de la sécurité devrait être exécutée périodiquement pendant les opérations courantes et pourra être mise en oeuvre par le biais de la collecte de la configuration et de l'analyse de la sécurité des bases de référence.

4) Gestion des conflits en matière de configuration de la sécurité

Dans un environnement en nuage avec partage des ressources, les défaillances imputables à l'administrateur de la sécurité ou dues à d'autres raisons risquent de compromettre la configuration de la sécurité, ce qui peut entraîner des vulnérabilités au niveau de l'environnement de l'informatique en nuage. Les fournisseurs CSP devraient appliquer des mesures efficaces pour déceler les conflits au niveau de la configuration de la sécurité et mettre en place un processus de gestion des conflits concernant la configuration de la sécurité ainsi que des mécanismes de recherche.

Le processus de gestion des conflits en matière de configuration de la sécurité devrait comporter les éléments suivants: alarme en cas de conflit, analyse des conflits (avec analyse des motifs et des influences), traitement des conflits et rapport sur les résultats.

5) Gestion de la migration de la configuration de la sécurité

En cas de changement des ressources ou des services d'informatique en nuage (par exemple, expansion de la capacité de service, migration des machines VM, etc.), les fournisseurs CSP devraient prévoir des moyens d'adaptation dynamique de la configuration de la sécurité. Ainsi, en cas de migration VM, la migration automatique de la politique de configuration de la sécurité pourra être mise en oeuvre par le biais de la détection du statut de la migration, de l'adaptation automatique et du redéploiement de la politique initiale en matière de configuration de la sécurité, ce qui permettra de garantir la cohérence de la politique de configuration de la sécurité et le développement rapide dans l'environnement du nuage, tout en améliorant l'efficacité de la sécurité.

6) Gestion de l'isolation de la configuration de la sécurité

Dans un environnement informatique en nuage multilocataires, les fournisseurs CSP devraient procéder à une gestion rigoureuse de la classification des configurations de sécurité des clients CSC, et prendre des mesures telles que l'authentification, le contrôle d'accès, etc., de façon à garantir l'isolation de la configuration de la sécurité entre différents clients CSC.

8.6 Traitement des événements de sécurité

Les fournisseurs CSP devraient mener certaines activités pour gérer les événements de sécurité dans l'environnement informatique en nuage, tels que les alarmes signalant des menaces, les vulnérabilité, les situations d'urgence, etc. Les fournisseurs CSP devraient également mettre en place des mesures techniques pour faciliter la détection, l'alarme et la gestion des événements de sécurité.

D'une manière générale, la procédure de traitement des événements de sécurité dans l'environnement informatique en nuage comprend les étapes suivantes: détection, analyse, élimination, vérification, signalement et enregistrement. Les fournisseurs CSP devraient expressément préciser les personnes responsables de chaque étape.

8.6.1 Détection

Les fournisseurs CSP devraient prendre des mesures pour suivre l'état de la sécurité de la plate-forme en nuage visé au § 8.3 et se doter des moyens permettant d'envoyer rapidement des alarmes chaque fois que des événements de sécurité se produisent. Ils devraient faire en sorte que les alarmes puissent être envoyées à la personne désignée, par exemple au responsable de la sécurité de la plate-forme informatique en nuage. Les alarmes pourront être envoyées par courrier électronique, par appel téléphonique ou par SMS (service de messages courts), etc. Les fournisseurs CSP devraient s'assurer du suivi de tous les événements de sécurité de tous types décrits dans la clause de sécurité de l'accord SLA.

8.6.2 Analyse

Les fournisseurs CSP devraient confirmer les événements de sécurité après la réception d'alarmes, puis les analyser et les diagnostiquer afin de déterminer les types d'événements, leurs causes et les mesures à prendre pour les traiter. Les fournisseurs CSP pourront si nécessaire se mettre en rapport avec les clients CSC aux fins d'assistance.

8.6.3 Elimination

Les fournisseurs CSP devraient prendre des mesures de traitement en fonction du type et du niveau d'un événement de sécurité, afin de réduire le plus possible les incidences de ces événements. Les fournisseurs CSP devraient se reporter aux activités de sécurité visées aux § 8.7, 8.8 et 8.9, qui comprennent, sans que cette liste soit limitative, les activités suivantes:

1) Dans une situation d'urgence liée à la sécurité, les fournisseurs CSP devraient prendre des mesures en fonction des plans d'intervention en cas d'urgence.
2) En cas de vulnérabilité liée à la sécurité, les fournisseurs CSP devraient prendre des mesures en fonction de la mise à jour des correctifs.
3) En cas de faille de la configuration, les fournisseurs CSP devraient prendre des mesures en fonction de de la sécurisation de la gestion de la configuration.

Les fournisseurs CSP devraient surveiller et évaluer de manière dynamique les événements de sécurité et informer les clients CSC des informations connexes et de l'état d'avancement du traitement.

8.6.4 Vérification

Après avoir traité les événements de sécurité, les fournisseurs CSP devraient analyser de manière approfondie les raisons et les situations susceptibles d'être à l'origine des événements de sécurité et vérifier si les systèmes d'autres clients CSC présentent des vulnérabilités analogues pouvant avoir déclenché les mêmes événements de sécurité. Si la vulnérabilité existe, les fournisseurs CSP devraient en informer immédiatement les clients CSC concernés et prendre les mesures correspondantes. La notification ne devrait pas concerner les données personnelles d'autres clients CSC.

8.6.5 Rapport et enregistrement

Les fournisseurs CSP devraient élaborer un rapport sur le traitement des événements de sécurité portant sur le comportement, les causes, les mesures de gestion des événements de sécurité, etc., et l'envoyer aux clients CSC concernés, dans les délais fixés dans la clause de sécurité de l'accord SLA. Les fournisseurs CSP devraient enregistrer les informations sur les événements de sécurité pour inspection et audit ultérieurs. Les rapports appropriés pourront être transmis aux clients CSP affectés ainsi qu'aux tiers effectuant les audits (agissant en qualité de partenaires CSN).

8.7 Mise à jour des correctifs

8.7.1 Responsabilités

Les fournisseurs CSP devraient optimiser le processus de gestion des correctifs de la plate-forme du nuage afin de réduire les risques potentiels dus aux vulnérabilités et protéger la stabilité de fonctionnement des plates-formes et services en nuage.

En ce qui concerne l'informatique en nuage, la gestion des correctifs devrait être mise en oeuvre collectivement entre fournisseurs CSP et clients CSC.

1) Responsabilités incombant aux fournisseurs CSP:
   - Suivre de près les versions des systèmes d'exploitation miroir présentant des vulnérabilités et trouver en temps voulu les correctifs les plus récents.
   - Tester la sécurité et l'adaptabilité des correctifs.
   - Mettre à jour les correctifs du système d'exploitation miroir et créer les fichiers d'image les plus récents.
   - Informer les clients CSC et les aider à achever la mise à jour des correctifs, tout en veillant à ce que la même vulnérabilité n'apparaisse plus.
   - Effectuer le test des effets de ces fichiers d'image les plus récents en créant une nouvelle machine virtuelle.
2) Responsabilités incombant aux clients CSC:
   - Aider les fournisseurs CSP à suivre de près les versions présentant des vulnérabilités et à trouver les correctifs les plus récents.
   - Mettre à jour en temps voulu les correctifs des machines virtuelles en fonction des informations communiquées par les fournisseurs CSP.

En fonction du mode de service de l'informatique en nuage, par exemple IaaS, PaaS et SaaS, le fournisseur CSP est uniquement responsable de la ressource qu'il contrôle lui-même, de même que le client CSC. En ce qui concerne l'infrastructure IaaS, les fournisseurs CSP devraient être responsables de la mise à niveau des correctifs de l'infrastructure informatique en nuage et les clients CSC du système d'exploitation invité, du logiciel d'application, etc., qui sont contrôlés par les clients CSC.

8.7.2 Processus de mise à niveau des correctifs de sécurité

Les composantes de la plate-forme en nuage qui nécessitent des correctifs sont le logiciel de virtualisation, les systèmes d'exploitation, l'équipement réseau, l'équipement de sécurité, les serveurs de bases de données, les terminaux de gestion et les autres composantes de la plate-forme en nuage. Le processus en circuit fermé de la mise à niveau des correctifs comporte quatre étapes, comme indiqué ci-dessous, qui pourraient aider les fournisseurs CSP à assurer la mise en oeuvre rapide des correctifs apportés à leur plate-forme en nuage.

1) Collecte d'informations sur les correctifs

Les fournisseurs CSP devraient recueillir des informations sur les correctifs sur le site web officiel de mise à jour des correctifs du fournisseur, utiliser les outils de mise à jour automatique des correctifs fournis par les fournisseurs ou recourir à d'autres moyens visant à garantir l'intégrité des exigences en matière de correctifs. Les fournisseurs CSP devraient procéder à une analyse des correctifs ainsi recueillis, rechercher et enregistrer les vulnérabilités des systèmes et applications existants, évaluer les effets et risques potentiels des correctifs et déterminer l'urgence et l'importance des correctifs.

2) Tests concernant les correctifs

Les fournisseurs CSP devraient procéder à un test des correctifs pour vérifier la sécurité, la compatibilité et la stabilité des correctifs. Ils devraient mettre en place un environnement de test pour l'émulation de la plate-forme ou des systèmes cibles avant l'étape de la correction. A l'issue des tests, un rapport devrait être établi, qui pourrait indiquer s'il convient de distribuer ou non les correctifs. Le rapport de test fournit également des directives techniques détaillées concernant les étapes de la correction et le programme d'invalidation. Ce rapport devrait décrire de manière détaillée les correctifs, pour aider les ingénieurs à mieux comprendre les fonctions et opérations des correctifs, les effets sur les systèmes et applications, par exemple les problèmes créés par les correctifs, les systèmes affectés, les fichiers affectés, la question de savoir si le système ou l'application devrait être rechargé ou non, etc.

3) Mise à jour de correctifs

Les fournisseurs CSP devraient établir un plan opérationnel en vue de la mise à jour des correctifs comprenant les étapes opérationnelles détaillées, en fonction du rapport de test des correctifs. Il convient également de formuler un plan d'urgence prévoyant la sauvegarde du système et des données, la commutation des applications, le contrôle de synchronisation de la distribution des correctifs, la désinstallation des correctifs et l'invalidation du système, en cas de défaillance des correctifs. En ce qui concerne la distribution de correctifs à grande échelle, les fournisseurs CSP devraient demander à l'avance l'appui technique des fournisseurs, afin d'améliorer la capacité de traitement d'urgence dans les situations imprévues.

Les fournisseurs CSP devraient également faire preuve de transparence vis-à-vis des clients CSC lorsque les correctifs sont distribués sur la plate-forme du nuage et communiquer de manière claire avec les clients CSC avant d'apporter les corrections. Les fournisseurs CSP devraient éviter d'influencer de quelque manière que ce soit les services offerts aux clients CSC, en adoptant à cet effet des mesures appropriées conjointement avec les clients CSC.

4) Vérification des correctifs

Après la distribution des correctifs, les fournisseurs CSP devraient vérifier périodiquement ces derniers au moyen des outils de gestion des correctifs, afin de veiller à ce que les correctifs de l'ensemble de la plate-forme en nuage soient les correctifs les plus récents. Le document contenant les enregistrements des correctifs devrait être actualisé régulièrement et être archivé aux fins des audits de sécurité ultérieurs.

Le temps d'attente entre la collecte et la mise à jour des correctifs et l'obligation d'approbation de la mise à jour des correctifs par les clients CSC devrait être expressément indiqué dans l'accord SLA, en fonction du type de priorité du correctif (priorité critique, élevée, moyenne et faible, par exemple).

On trouvera ci-dessous un exemple de processus de mise à jour des correctifs de sécurité, notamment la mise à jour de la machine virtuelle et de ses fichiers d'image. Au cours de ce processus, si les versions les plus récentes des correctifs sont distribuées, les fournisseurs CSP testeront la sécurité et l'adaptabilité de ces correctifs. En outre, les clients CSC ont pour tâche de trouver et de collecter les correctifs les plus récents. Une fois que ces correctifs les plus récents auront été testés avec succès, les fournisseurs CSP informeront les clients CSC et leur demanderont de mettre à jour ces correctifs. Parallèlement, les fournisseurs CSP actualiseront les correctifs des fichiers d'image actuels. Les fournisseurs CSP pourront alors créer une nouvelle machine virtuelle avec ces nouveaux fichiers d'image. Les fournisseurs CSP procéderont également à un balayage spécifique afin de veiller à ce que les clients CSC aient mis à jour avec succès ces correctifs.

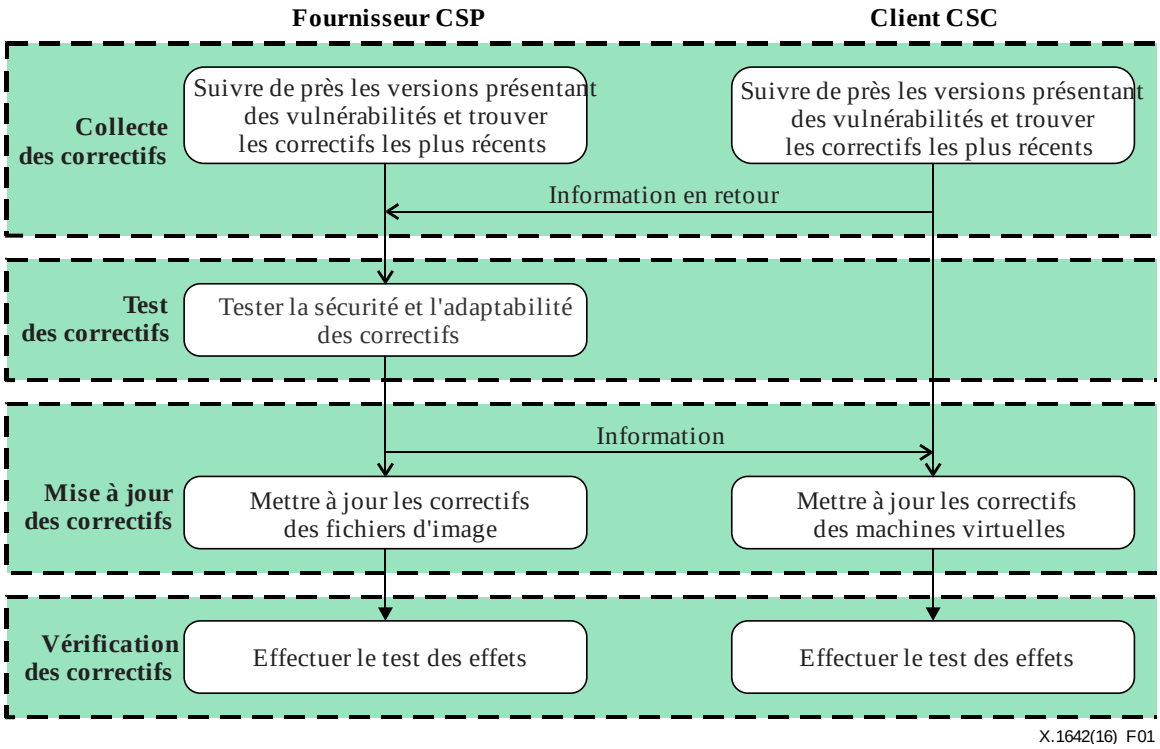

Figure 1 – Exemple de processus de mise à niveau des correctifs de sécurité

8.8 Sécurisation de la gestion de la configuration

Les fournisseurs CSP devraient exécuter les contrôles de sécurité de la gestion de configuration de la plate-forme en nuage, de la configuration du réseau et des paramètres des différentes composantes des applications, de manière à réduire les risques opérationnels dus aux erreurs de configuration ou à une utilisation abusive et à favoriser la sécurité et la stabilité de l'environnement informatique en nuage.

La gestion de la configuration comprend généralement la gestion des modifications de la configuration et la gestion des versions. Les fournisseurs CSP devraient prendre des mesures pour faire en sorte que les modifications et les versions de la configuration ont été suivies de près et enregistrées. Afin de faciliter la gestion de la configuration, on crée habituellement une base de données de gestion de la configuration intégrée, qui comprend les enregistrements actuels et les enregistrements chronologiques de tous les fichiers de configuration, la politique de sécurité et les profils d'application de chaque élément et composante de l'informatique en nuage. Les fournisseurs CSP devraient protéger cette base de données contre tout accès non autorisé, toute fuite d'informations, etc.

La sécurité de la gestion de la configuration comporte les mesures suivantes:

1) Audit de la gestion de la configuration

   L'audit de la gestion de la configuration vise à faire en sorte que les exigences concernant les modifications et les versions de la configuration ont été mises en oeuvre de manière efficace et efficiente. Cette mesure aidera les fournisseurs CSP à vérifier que chaque élément de la configuration est correct, cohérent, complet, valable et traçable. L'audit de la gestion de la configuration devrait être exécuté périodiquement pendant les opérations courantes.

   Tous les journaux de l'accès de l'utilisateur, des modifications, des archives et de l'extraction devraient être enregistrés et archivés pour audit en ligne et hors ligne.

   En outre, le rapport de l'audit de gestion de la configuration relatif aux clients CSC ou à leurs services devrait être visible pour les clients CSC, de façon à leur permettre de superviser les mesures de sécurité et l'efficacité des fournisseurs CSP.

2) Suivi de la gestion de la configuration

Les fournisseurs CSP devraient suivre de près toutes les alternances et autres opérations des fichiers de configuration de l'environnement informatique en nuage dans son intégralité, afin d'empêcher tout accès non autorisé, toute fuite et toute modification illégale ainsi que toute erreur de configuration.

3) Protection de la base de données de gestion de la configuration

Les fournisseurs CSP devraient effectuer une maintenance et une gestion précises de la base de données de gestion de la configuration, par exemple l'attribution de l'autorité fondée sur le rôle, la suppression des déchets, l'audit régulier, la sauvegarde périodique, etc.

8.9 Plans d'intervention en cas d'urgence

Il est indispensable de veiller à ce que les systèmes informatiques en nuage puissent être exploités efficacement par les fournisseurs CSP, sans interruption excessive à la suite d'un incident de sécurité. Un plan d'intervention en cas d'urgence permet de satisfaire à cette exigence moyennant la mise en place d'un programme, de procédures et de mesures techniques efficaces.

Afin de limiter les conséquences des incidents de sécurité sur les plates-formes et les services informatiques en nuage, le plan d'intervention en cas d'urgence des fournisseurs CSP devrait fournir des directives précises aux opérateurs et trouver un compromis entre le niveau de détail et le degré de souplesse. L'élaboration et la gestion d'un plan d'intervention en cas d'urgence constituent un cycle s'inscrivant dans un processus d'amélioration continu composé de trois phases: phase de développement, phase de test et de mise en oeuvre et phase de maintenance.

8.9.1 Phase de développement

Il convient avant tout d'adopter des méthodes d'analyse quantitative et qualitative, afin de procéder à une évaluation complète des risques et à une analyse d'impact sur les activités (BIA) exhaustive des systèmes informatiques en nuage. Par la suite, il sera possible d'obtenir les principales fonctionnalités et composantes du système et de déterminer les conséquences de différents incidents de sécurité. Sur cette base, conformément à la clause de sécurité de l'accord SLA conclu entre les fournisseurs CSP et les clients CSC, il sera possible de définir les prescriptions réglementaires et de formuler l'objectif de rétablissement de l'intervention en cas d'urgence, tel que la portée de l'objectif de point de reprise (RPO) et l'objectif de durée de reprise (RTO). De plus, il convient également de tenir compte des caractéristiques du service en nuage et de la classification des incidents lors de l'élaboration d'un plan d'intervention en cas d'urgence.

Le plan d'intervention en cas d'urgence comprend les éléments suivants:

1) Notification: il convient d'élaborer une procédure de notification afin d'informer l'équipe d'intervention, le personnel de direction et les clients CSC concernés dès qu'un incident de sécurité se produit.

2) Classification et évaluation des événements de sécurité: l'équipe d'intervention en cas d'urgence devrait évaluer la sécurité d'un incident de sécurité afin d'en déterminer la catégorie et le type.

3) Lancement: après la classification et l'évaluation des événements de sécurité, les fournisseurs CSP et les clients CSC doivent d'urgence activer le programme d'intervention correspondant qui a été établi au préalable.

4) Mesures: une fois que le programme d'intervention a été activé, il convient de prendre immédiatement des mesures de protection pour supprimer les conséquences des incidents de sécurité. En outre, il convient de mener des opérations de rétablissement dès que les incidents ont été efficacement maîtrisés.

5) Elimination postérieure: à la suite d'une intervention d'urgence, il est important de tirer des conclusions sur les dernières interventions effectuées en cas d'urgence, qui comprennent les mesures destinées à analyser et à récapituler les raisons de l'incident et à procéder à une évaluation des pertes et de l'efficacité ainsi que de l'efficience du plan d'intervention en cas d'urgence.

En outre, certains éléments revêtent une importance essentielle, à savoir:

1) Membres de l'équipe d'intervention en cas d'urgence, responsabilités spécifiques et coordonnées de chaque membre de l'équipe. D'une manière générale, l'équipe d'intervention en cas d'urgence comprend les cadres, le personnel de l'entreprise ainsi que le personnel technique et administratif.
2) Résultats de l'analyse d'impact sur les activités concernant les relations entre les différentes parties du système informatique en nuage, le niveau de priorité des composantes essentielles, etc.
3) Procédures et listes de contrôle concernant les critères de rétablissement du système informatique en nuage.
4) Inventaire du matériel, des logiciels, des micrologiciels et des autres ressources destinées à appuyer les opérations courantes des fournisseurs CSP, chaque entrée contenant des spécifications telles que les versions, les quantités, etc.
5) Coordonnées des clients CSC et procédures d'intervention négociées par les fournisseurs CSP et les clients CSC, conformément à la clause de sécurité de l'accord SLA, de manière à limiter le plus possible les pertes pour les clients CSC lors d'un accident de sécurité.
6) En général, les fournisseurs CSP ne pourront pas avoir le privilège d'accéder aux données privées des clients CSC, à moins qu'ils n'aient obtenu l'autorisation d'un client CSC. En cas d'urgence lancée par un client CSC, celui-ci aura peut-être besoin de l'assistance du fournisseur CSP afin que l'intervention soit plus efficace, et accordera au fournisseur CSP l'autorisation pour les données. Dans le cadre de la conformité, le fournisseur CSP ne devrait pas faire un usage abusif de l'autorisation d'accéder aux données des clients CSC.

8.9.2 Phase de test et de mise en oeuvre

Afin de tester l'efficacité du plan d'intervention en cas d'urgence, les fournisseurs CSP devraient organiser des tests et des exercices dans le cadre du plan d'intervention en cas d'urgence, avec l'assistance du personnel concerné connaissant bien les procédures d'intervention. Les tests et les exercices devraient satisfaire aux exigences suivantes:

1) Les programmes de test, la formation et les exercices devraient être établis au préalable.
2) Le processus détaillé de test, de formation et d'exercice devrait être enregistré et des rapports de tests devraient être rédigés à cette fin.
3) Il est recommandé aux fournisseurs CSP et aux clients CSC de procéder collectivement à un test planifié chaque fois que des changements importants surviennent à l'intérieur ou à l'extérieur de l'informatique en nuage.

En cas d'incident de sécurité ou d'interruption des activités, le plan d'intervention en cas d'urgence devrait être rigoureusement appliqué une fois que les conditions de lancement ont été satisfaites et tous les journaux opérationnels devraient être enregistrés pendant l'ensemble du processus d'urgence. Par la suite, conformément à la clause de sécurité de l'accord SLA, les fournisseurs CSP devraient soumettre les rapports d'intervention aux clients CSC.

En fonction des résultats des tests, des exercices et de la mise en oeuvre, il conviendra de revoir le plan d'intervention en cas d'urgence de manière à en améliorer l'efficacité et la viabilité.

8.9.3 Phase de maintenance

Pour rester efficace, le plan d'action en cas d'urgence devrait en permanence être maintenu dans un état prêt qui pourrait tenir compte des exigences des systèmes informatiques en nuage, de la modification de l'accord SLA, des changements de configuration et des changements de personnel. D'une manière, le plan devrait être réexaminé chaque année pour tenir compte de l'évolution de l'environnement réel de l'informatique en nuage. La modification du plan est fondée sur les éléments suivants:

1) Changements concernant les locaux, les installations, les ressources et les services.
2) Modifications concernant la clause de sécurité de l'accord SLA, la configuration de la sécurité critique, les mises à niveau importantes des correctifs et les membres de l'équipe centrale.
3) Evaluation de l'efficacité du plan sur la base des relevés détaillés de la mise en oeuvre effective du plan pendant les tests et les accidents de sécurité.

8.10 Sauvegarde

La capacité de sauvegarde constitue une question importante pour les clients CSC et les fournisseurs CSP dans l'environnement informatique en nuage. Avant de mener à bien les activités de sauvegarde, les fournisseurs CSP doivent tenir compte de certaines spécifications, à savoir:

– Stratégie de sauvegarde pour chaque client ou tel ou tel service en nuage.
– Méthode de stockage, avec chiffrement ou non.
– Emplacement du stockage, y compris stockage local et/ou à distance.
– Périodes de conservation pour les données de sauvegarde.
– Procédures de test des données de sauvegarde.

Avant de choisir un fournisseur CSP, le client CSC devrait confirmer si ce fournisseur CSP est à même de satisfaire la clause de sécurité de l'accord SLA, y compris la capacité de sauvegarde. Si les fournisseurs CSP ne prévoient pas de capacité de sauvegarde, les clients CSC devraient dûment envisager une stratégie et une mise en oeuvre de sauvegarde. Dans le cas contraire, si les fournisseurs CSP prévoient une capacité de sauvegarde, les clients CSC devraient coopérer avec les fournisseurs CSP afin de mener à bien les opérations de sauvegarde.

Les fournisseurs CSP devraient communiquer aux clients CSC les données essentielles concernant le mécanisme de sauvegarde. Lorsqu'ils examinent la sauvegarde, les fournisseurs CSP devraient examiner les spécifications de façon à répondre aux besoins suivants des clients CSC:

1) Stratégie de sauvegarde: étant donné que chaque client CSC a des besoins individuels dans la sauvegarde, il convient de tenir dûment compte des facteurs correspondants, à savoir:
   – Objectif de point de reprise (RPO) et objectifs de durée de reprise (RTO) raisonnables: L'objectif RPO désigne le laps de temps écoulé entre deux activités de sauvegarde consécutives, tandis que l'objectif RTO indique combien de temps il faut pour retourner à une sauvegarde.
   – Politique de conservation raisonnable: Cette politique devrait préciser le nombre de copies d'une sauvegarde.
   – Combinaison raisonnable de sauvegarde au niveau des fichiers et de sauvegarde au niveau de la machine virtuelle: Cette combinaison devrait correspondre à un coût d'investissement optimal, qui est fondé sur l'objectif RPO et l'objectif RTO.
   – Combinaison raisonnable de sauvegarde sur site et de sauvegarde hors site: La sauvegarde sur site est stockée sur le site local, ce qui permettrait de répondre à la nécessité d'un rétablissement rapide après une catastrophe. La sauvegarde hors site est stockée sur un site distant, ce qui est nécessaire pour faire face à une catastrophe majeure.

La combinaison dépend des exigences de la clause de sécurité de l'accord SLA et du coût de l'investissement.

- Procédures de test régulières concernant le rétablissement: Le test de rétablissement constitue la meilleure méthode pour vérifier la validité d'une sauvegarde.

2) Organisation des tâches: Une fois que la stratégie de sauvegarde a été déterminée, les fournisseurs CSP devraient procéder à une organisation appropriée des tâches concernant les opérations de sauvegarde. Pour réduire les incidences sur la qualité de fonctionnement de l'infrastructure informatique en nuage, l'organisation des tâches de sauvegarde devrait dépendre des besoins des clients CSC en matière de sauvegarde, de la configuration du trafic de réseau et de la capacité de sauvegarde des fournisseurs CSP.

3) Procédure de vérification de la validation de la sauvegarde: Une copie des données complète et correcte signifie que l'opération de sauvegarde est réussie. En général, les procédures devraient comporter les deux principales étapes suivantes:

   - Utilisation d'une fonction de hachage unidirectionnelle pour vérifier que la sauvegarde est conforme aux données d'origine. Si la sauvegarde est la même que l'original, il convient de passer à l'étape suivante. De plus, une méthode fondée sur une signature numérique pourrait être utilisée pour vérifier l'opérateur de la sauvegarde, ce qui pourra offrir certains avantages pour la gestion de l'opération de sauvegarde.
   - Réalisation d'un test de rétablissement pour la sauvegarde. En raison de l'évolution constante de l'environnement informatique en nuage, il est indispensable de procéder à des tests de rétablissement périodiques.

4) Nécessité de faire preuve de prudence concernant les instantanés de la machine virtuelle: dans un scénario d'informatique en nuage, la méthode des instantanés offre un moyen de retour-arrière rapide et aisé, qui pourra faire office de méthode de sauvegarde dans une certaine mesure. Cependant, la méthode des instantanés ne devrait pas être utilisée fréquemment, et ce pour les raisons suivantes:

   - Les instantanés permettent de multiplier les mêmes données et de les écrire dans différents fichiers d'instantanés, ce qui pourrait aisément entraîner une grave dégradation de la qualité de fonctionnement et un taux d'occupation rapide du stockage dans les systèmes informatiques en nuage.
   - Afin de réduire le taux d'occupation du stockage, on configure souvent une chaîne d'instantanés d'une machine virtuelle d'origine, afin qu'elle contienne simplement la différence par rapport au premier instantané. Une fois que le premier instantané est détruit, les instantanés successifs finiront par être non valides. Le risque pour la sécurité est accru à mesure que le taux d'instantanés successifs augmente.

8.11 Audit de sécurité interne

Etant donné qu'il existe une grande diversité d'audits de sécurité, la présente Recommandation ne porte que sur l'audit de sécurité interne du point de vue de la sécurité opérationnelle. Un audit de sécurité fiable et objectif permet de faire en sorte que les activités de gestion des risques opérationnels ont été testées et examinées de manière approfondie, de manière à accroître la transparence des services informatiques en nuage, voire à satisfaire les prescriptions réglementaires.

8.11.1 Conditions requises pour l'audit de sécurité

Pour garantir l'objectivité et la fiabilité de l'audit de sécurité, les fournisseurs CSP et les clients CSC devraient négocier de manière à parvenir à un accord sur l'utilisation d'un cadre commun d'assurance de certification et de contrôle IT ainsi que sur les moyens de collecter, de stocker et d'échanger le journal d'audit (journaux système, rapports d'activité, configurations du système, par exemple).

Conformément à la clause de sécurité de l'accord SLA conclu entre les fournisseurs CSP et les clients CSC, l'audit de sécurité devrait être planifié et ciblé pour satisfaire certaines conditions requises.

1) Equipe et fonction: Premièrement, les membres de l'équipe d'audit devraient comprendre les cadres supérieurs et le personnel des différents services de l'entreprise (personnel administratif et personnel technique), de façon à garantir l'équité et la planification des ressources pendant le processus d'audit. Deuxièmement, l'objectif de l'audit devrait être de vérifier l'architecture de gestion de la sécurité des fournisseurs CSP et/ou des clients CSC et de valider l'efficacité et le bien-fondé des mesures de contrôle des risques. Troisièmement, le processus d'audit devrait être contrôlé par l'équipe d'audit et être conforme au déroulement des tâches normalisé. Enfin, l'audit de sécurité devrait être effectué à plusieurs reprises et au moment voulu.

2) Conditions requises pour le processus d'audit: Premièrement, et compte tenu de ce qui précède, les activités d'audit devraient être dûment consignées et planifiées de manière à éviter toute interruption du processus opérationnel des fournisseurs CSP et des clients CSC. Deuxièmement, la portée des objectifs de l'audit et les ressources nécessaires devraient être clairement définies et leur disponibilité devrait être garantie. Enfin, toutes les procédures et prescriptions relatives à l'audit devraient être documentées, de même que les responsabilités des membres de l'équipe d'audit.

3) Protection des outils d'audit: L'utilisation d'outils d'audit devrait être restreinte et normalisée de façon à éviter toute utilisation abusive des ressources informatiques en nuage.

8.11.2 Prescriptions particulières concernant l'audit

Par rapport aux procédures d'audit de sécurité des systèmes d'information classiques, il est tout particulièrement demandé aux membres de l'équipe d'audit de bien connaître les problèmes inhérents à la virtualisation et à d'autres technologies liées à l'informatique en nuage. Parallèlement, la catégorie d'audit doit être développée, pour passer des journaux de sécurité traditionnels à l'exploitation et à la tenue à jour des données, des données commerciales, voire de l'emplacement de stockage des données des utilisateurs. Les éléments de l'audit comprennent, sans toutefois que cette liste soit limitative, les éléments suivants:

1) Audit de sécurité de virtualisation: Les principales exigences en matière d'audit comprennent les moyens de chiffrement et de contrôle de l'intégrité pour les fichiers d'images virtuels, l'isolation et le renforcement des différentes machines virtuelles, le contrôle d'accès et la migration des machines virtuelles, le suivi des processus des machines virtuelles et l'inspection de vulnérabilité dans les machines virtuelles, le suivi et les mesures du trafic interne au niveau du réseau virtualisé.

2) Audit de sécurité de l'architecture et des composantes de la plate-forme en nuage: Il est primordial de procéder à un audit du caractère rationnel et de l'efficacité des mesures de prévention, et notamment la politique de répartition des domaines de sécurité, la redondance de sécurité de l'architecture et des composantes principales du réseau, l'analyse des vulnérabilités et le renforcement de la sécurité, l'assemblage et la distribution des correctifs et les configurations du système de prévention des intrusions (IPS)/du système de détection des intrusions (IDS), des pare-feux et des dispositifs de sécurité de virtualisation.

3) Audit de l'exploitation, de la maintenance et du comportement de l'entreprise: Les prescriptions en matière d'audit sont principalement axées sur les registres d'exploitation et de maintenance, les journaux d'accès de l'entreprise, l'accès aux données et l'inspection du comportement de l'entreprise.

4) Audit de gestion de l'identité et de l'accès (IAM) et du contrôle d'accès: Les prescriptions en matière d'audit sont d'une importance capitale pour assurer le bon fonctionnement de l'environnement informatique en nuage, qui comprend la conception et le déploiement de l'authentification multifactorielle, du contrôle d'accès, de l'authentification unique (SSO), de la séparation des tâches et de la gestion des utilisateurs disposant de privilèges.

5) Audit de gestion des clés et du chiffrement des données: Etant donné que le chiffrement constitue le principal mécanisme de protection des données dans l'environnement informatique en nuage, quel que soit le modèle de service – IaaS, PaaS, voire SaaS – les prescriptions en matière d'audit devraient comprendre la mise en oeuvre et le traitement de la gestion des clés et du chiffrement des données.

6) Audit de gestion des situations d'urgence et d'intervention en cas d'urgence: Les prescriptions en matière d'audit sont principalement axées sur un plan d'urgence, une gestion centralisée des incidents de sécurité et une analyse de corrélation entre les différents événements de sécurité.

Bibliographie

[b-UIT-T E.409] Recommandation UIT-T E.409 (2004), *Organisation en cas d'incident et prise en charge des incidents relatifs à la sécurité: Lignes directrices à l'intention des organisations de télécommunication*.

[b-UIT-T X.810] Recommandation UIT-T X.810 (1995) | ISO/CEI 10181-1:1996, *Technologies de l'information – Interconnexion des systèmes ouverts – Cadres de sécurité pour les systèmes ouverts: Vue d'ensemble.*

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

[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-UIT-T Y.3510] Recommandation UIT-T Y.3510 (2016), *Exigences relatives à l'infrastructure de l'informatique en nuage.*

[b-ISO/CEI DIS 19086-1] ISO/CEI DIS 19086-1:2016, *Technologies de l'information – Informatique en nuage – Cadres et technologies applicables à l'accord de niveau de service (SLA) – Partie 1: Vue d'ensemble et concepts.*

[b-ISO/CEI 20000-1] ISO/CEI 20000-1:2011, *Technologies de l'information – Gestion des services – Partie 1: Exigences du système de gestion des services.*

[b-ISO/CEI 27000] ISO/CEI 27000:2012, *Technologies de l'information – Techniques de sécurité – Systèmes de gestion de la sécurité de l'information – Vue d'ensemble et vocabulaire.*

[b-ISO/CEI DIS 27017] ISO/CEI DIS 27017:2015, *Technologies de l'information – Techniques de sécurité – Code de bonne pratique pour les contrôles de sécurité de l'information sur la base de la norme ISO/CEI 27002 pour les services en nuage.*

[b-ISO 27729] ISO 27729:2012, *Information et documentation – Code international normalisé des noms (ISNI).*

[b-NIST-SP-800-30] Publication spéciale du NIST 800-30 Rév. 1 (2012), *Guide pour l'évaluation des risques.*

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