Union internationale des télécommunications

UIT-T

SECTEUR DE LA NORMALISATION
DES TÉLÉCOMMUNICATIONS
DE L'UIT

X.1605

(03/2020)

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

Sécurité de l'informatique en nuage – Conception de la sécurité de l'informatique en nuage

Exigences de sécurité pour les infrastructures en tant que service (IaaS) publiques dans l'informatique en nuage

Recommandation UIT-T X.1605

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 (1)	
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 (1)	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 spam	X.1230–X.1249
Gestion des identités	X.1250–X.1279
APPLICATIONS ET SERVICES SÉCURISÉS (2)	
Communications d'urgence	X.1300–X.1309
Sécurité des réseaux de capteurs ubiquitaires	X.1310–X.1319
Sécurité des réseaux électriques intelligents	X.1330–X.1339
Courrier certifié	X.1340–X.1349
Sécurité de l'Internet des objets (IoT)	X.1360–X.1369
Sécurité des systèmes de transport intelligents	X.1370–X.1389
Sécurité de la technologie des registres distribués	X.1400–X.1429
Sécurité de la technologie des registres distribués	X.1430–X.1449
Protocoles de sécurité (2)	X.1450–X.1459
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
COMMUNICATION QUANTIQUE	X.1700–X.1729

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

Recommandation UIT-T X.1605

Exigences de sécurité pour les infrastructures en tant que service (IaaS) publiques dans l'informatique en nuage

Résumé

Les plates-formes d'infrastructure en tant que service (IaaS) et les services virtualisés sont confrontés à des problèmes et des menaces différents, et peut-être plus nombreux, par rapport aux infrastructures et aux applications traditionnelles des technologies de l'information. Les plates-formes IaaS qui utilisent en partage des services de calcul, de stockage et de réseau ont des besoins en matière de protection adaptés aux menaces propres à l'environnement IaaS. La Recommandation UIT-T X.1605 vise à fournir des informations concernant les exigences de sécurité pour les infrastructures IaaS publiques, afin d'aider les fournisseurs d'infrastructures IaaS à améliorer la sécurité des plates-formes IaaS au cours des étapes de planification, de construction et d'exploitation.

Historique

Édition	Recommandation	Approbation	Commission d'études	ID unique*
1.0	UIT-T X.1605	26-03-2020	2	11.1002/1000/14094

Mots clés

Informatique en nuage, IaaS, exigence de sécurité, ressources virtuelles.

* Pour accéder à la Recommandation, reporter cet URL http://handle.itu.int/ dans le champ adresse de 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 on considère que la Recommandation est respectée lorsque toutes ces dispositions sont observées. Le futur d'obligation et les autres moyens d'expression de l'obligation comme le verbe "devoir" ainsi que leurs formes négatives servent à énoncer des prescriptions. L'utilisation de ces formes ne signifie pas qu'il est obligatoire de respecter la Recommandation.

DROITS DE PROPRIÉTÉ INTELLECTUELLE

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

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

TABLE DES MATIÈRES

		Page
1	Domaine d'application	1
2	Références	1
3	Définitions	1
	3.1 Termes définis ailleurs	1
	3.2 Termes définis dans la présente Recommandation	2
4	Abréviations et acronymes	2
5	Conventions	3
6	Généralités	3
7	Problèmes de sécurité relatifs à l'environnement IaaS	5
8	Exigences de sécurité pour la couche d'accès d'une infrastructure IaaS	6
	8.1 Exigences de sécurité pour l'accès web	6
	8.2 Exigences de sécurité pour l'accès API	7
9	Exigences de sécurité pour la couche service d'une infrastructure IaaS	7
	9.1 Exigences de sécurité pour le service de calcul	7
	9.2 Exigences de sécurité pour le service de stockage	8
	9.3 Exigences de sécurité pour le service de réseau	8
10	Exigences de sécurité pour la couche ressources d'une infrastructure IaaS	9
	10.1 Exigences de sécurité pour la représentation abstraite et le contrôle des ressources	9
	10.2 Exigences de sécurité pour les ressources physiques	10
11	Exigences relatives à la gestion de la sécurité	11
	11.1 Gestion IdM et contrôle d'accès	12
	11.2 Audit de sécurité	12
	11.3 Gestion des vulnérabilités	13
	11.4 Intervention en cas d'urgence	14
	11.5 Reprise après sinistre	14
	11.6 Sauvegarde	15
Bibliographie		16

Recommandation UIT-T X.1605

Exigences de sécurité pour les infrastructures en tant que service (IaaS) publiques dans l'informatique en nuage

1 Domaine d'application

La présente Recommandation contient une analyse des problèmes de sécurité auxquels sont confrontés les fournisseurs d'infrastructures en tant que service (IaaS) dans les environnements IaaS ainsi que les exigences de sécurité pour les infrastructures IaaS publiques dans l'informatique en nuage. La présente Recommandation est applicable aux fournisseurs d'infrastructures IaaS publiques.

Elle constitue une description de haut niveau des exigences de sécurité pour la mise en œuvre des infrastructures IaaS. Les conseils détaillés de mise en œuvre n'entrent pas dans le cadre du présent document.

2 Références

La présente Recommandation se réfère à certaines dispositions des Recommandations UIT-T et textes suivants qui, de ce fait, en sont partie intégrante. Les versions indiquées étaient en vigueur au moment de la publication de la présente Recommandation. Toute recommandation ou autre référence étant sujette à révision, les utilisateurs de la présente Recommandation sont invités à rechercher la possibilité d'appliquer les éditions les plus récentes des Recommandations et autres références énumérées ci-dessous. La liste des Recommandations de l'UIT-T en vigueur est régulièrement publiée. La référence à un document figurant dans la présente Recommandation ne donne pas à ce document, en tant que tel, le statut de Recommandation.

[UIT-T X.1642] Recommandation UIT-T X.1642 (2016), *Lignes directrices relatives à la sécurité opérationnelle de l'informatique en nuage*.

[UIT-T Y.3502] Recommandation UIT-T Y.3502 (2014) | ISO/CEI 17789:2014, *Technologies de l'information – Informatique en nuage – Architecture de référence*.

[UIT-T Y.3513] Recommandation UIT-T Y.3513 (2014), *Informatique en nuage – Exigences fonctionnelles relatives à l'infrastructure en tant que service*.

[ISO/CEI 27002] ISO/CEI 27002:2013, *Technologies de l'information – Techniques de sécurité – Code de bonne pratique pour le management de la sécurité de l'information*.

[ISO/CEI 27031] ISO/CEI 27031:2011, *Technologies de l'information – Techniques de sécurité – Lignes directrices pour la préparation des technologies de la communication et de l'information pour la continuité d'activité*.

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, approvisionnées 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 via l'informatique en nuage invoquées à l'aide d'une interface définie.

3.1.3 client de services en nuage (CSC) [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 pour les 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 (CSP) [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 capacités de nuage fourni au client de services en nuage correspond à des capacités de type infrastructure.

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

3.1.8 vulnérabilité [b-NIST-SP-800-30]: faille dans un système d'information, dans les procédures de sécurité système, les contrôles internes ou la mise en œuvre, 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 et acronymes suivants:

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*)

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

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

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

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

DRO objet de reprise après sinistre (*disaster recovery object*)

DSP fournisseur de services numériques (*digital service provider*)

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

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

IdM gestion des identités (*identity management*)

I/O entrée/sortie (*input/output*)

NIC carte d'interface de réseau (*network interface card*)

OS système d'exploitation (*operating system*)

OTT over-the-top

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

RPO objectifs de point de reprise (*recovery point objectives*)

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*)

SQL langage de requête structuré (*structured query language*)

TIC technologies de l'information et de la communication

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

VLAN réseau local virtuel (*virtual local area network*)

VM machine virtuelle (*virtual machine*)

VXLAN réseau local extensible virtuel (*virtual extensible local area network*)

XSS script intersites (*cross site script*)

5 Conventions

L'expression "il est nécessaire" indique une exigence qui doit être strictement suivie et par rapport à laquelle aucun écart n'est permis pour pouvoir déclarer la conformité à la présente Recommandation.

L'expression "il est recommandé" indique une exigence qui est recommandée mais qui n'est pas absolument nécessaire. Cette exigence n'est donc pas indispensable pour déclarer la conformité.

L'expression "peut, à titre d'option," indique une exigence optionnelle qui est admissible, sans pour autant être en quoi que ce soit recommandée. Elle ne doit pas être interprétée comme l'obligation pour le fabricant de mettre en œuvre l'option et la possibilité pour l'opérateur de réseau ou le fournisseur de services de l'activer ou non, mais comme la possibilité pour le fabricant de fournir ou non cette option, sans que cela n'ait d'incidence sur la déclaration de conformité.

Dans la présente Recommandation et dans ses appendices, on trouve parfois les expressions doit, ne doit pas, devrait et peut. Celles-ci doivent respectivement être interprétées comme correspondant aux expressions il est nécessaire, il est interdit, il est recommandé et peut, à titre d'option. Lorsque ces expressions apparaissent dans un appendice ou dans des parties dans lesquelles il est expressément indiqué qu'elles sont données à titre d'information, elles doivent être interprétées comme étant dépourvues d'intention normative.

6 Généralités

Les infrastructures en tant que service (IaaS) forment une catégorie de services en nuage, pour laquelle les capacités fournies au client de services en nuage (CSC) correspondent à des capacités de type infrastructure [b-UIT-T Y.3500]. Les infrastructures IaaS permettent aux clients CSC d'utiliser les ressources de l'infrastructure en nuage (calcul, stockage et réseau) qui peuvent être configurées et libérées rapidement moyennant des efforts de gestion minimes. Les services IaaS publics permettent aux clients CSC de lancer leurs activités rapidement et facilement sans mettre en place de nouvelles infrastructures de technologies de l'information et de la communication (TIC) et les clients CSC peuvent utiliser ces ressources pour développer, héberger et exécuter des services et des applications à la demande et de manière souple et élastique, en fonction des besoins.

Sur la base du cadre de subdivision en couches élaboré en collaboration avec l'ISO/CEI et défini dans la Recommandation [UIT-T Y.3502] ainsi que du concept de haut niveau d'infrastructure IaaS, défini dans la Recommandation [UIT-T Y.3513], le concept de haut niveau des exigences de sécurité pour les infrastructures IaaS est illustré dans la Figure 6-1.

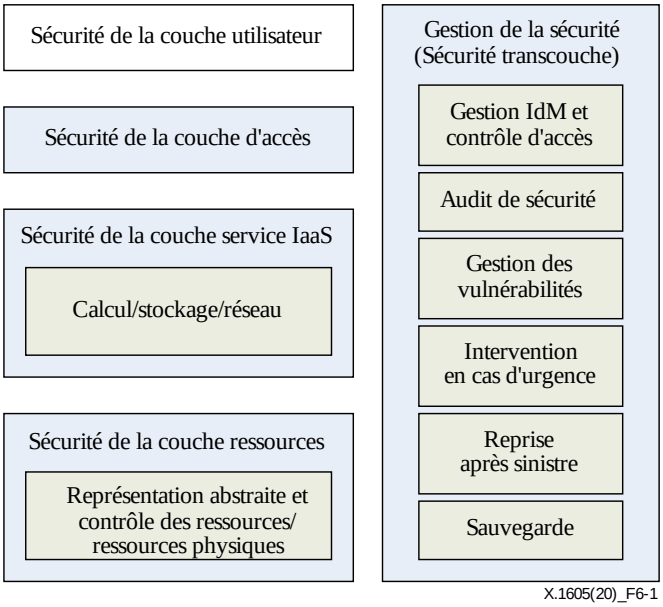

Figure 6-1 – Concept de haut niveau des exigences de sécurité pour les infrastructures IaaS

La couche utilisateur est l'interface utilisateur permettant au client CSC d'interagir avec le fournisseur de services en nuage (CSP). Les composantes fonctionnelles de la couche utilisateur comprennent les fonctions d'utilisateur, les fonctions relatives aux activités et les fonctions d'administrateur, qui interagissent avec les services en nuage assurés par le fournisseur CSP, effectuent des activités administratives relatives aux clients CSC et contrôlent les services en nuage. Suivant le partage des responsabilités entre le fournisseur CSP et les clients CSC, ces derniers devraient prendre en charge les mécanismes de sécurité de la couche utilisateur, car ils utilisent en général leurs propres outils ou systèmes pour accéder au service IaaS. Dans le cas contraire, si les outils ou systèmes de la couche utilisateur sont fournis par le fournisseur CSP, celui-ci doit fournir des outils ou systèmes conformes aux bonnes pratiques du secteur en matière de sécurité. Les exigences de sécurité pour la couche utilisateur sortent du cadre de la présente Recommandation.

La couche d'accès constitue une interface commune pour l'accès manuel et automatique aux capacités disponibles dans la couche service. Les composantes fonctionnelles de la couche d'accès comprennent le contrôle d'accès et la gestion des connexions. La couche d'accès est responsable de la présentation des capacités des services IaaS au moyen d'un ou plusieurs mécanismes d'accès tels que des interfaces web ou des interfaces de programmation d'application (API). Les exigences de sécurité pour la couche d'accès sont définies au paragraphe 8.

La couche service comprend la mise en œuvre des services IaaS fournis par le fournisseur CSP. Elle comprend et commande les composantes logicielles qui mettent en œuvre les services IaaS et permet de mettre les services à la disposition du client CSC au moyen de la couche d'accès. Les exigences de sécurité pour la couche service sont définies au paragraphe 9.

Les composantes de la couche ressources comprennent la représentation abstraite et le contrôle des ressources ainsi que les ressources physiques, comme indiqué dans la Recommandation [UIT-T Y.3502]. Les ressources virtualisées sont générées et contrôlées au moyen d'une abstraction logicielle. Les exigences de sécurité pour la couche ressources sont définies au paragraphe 10.

La gestion de la sécurité fournit les capacités fondamentales de gestion de la sécurité transcouche, qui sont mises en œuvre au niveau de la couche utilisateur, de la couche d'accès, de la couche service et de la couche ressources, comme indiqué plus haut. Les exigences relatives à la gestion de la sécurité concernant la gestion des identités et le contrôle d'accès, l'audit de sécurité, la gestion des vulnérabilités, l'intervention en cas d'urgence, la reprise après sinistre et la sauvegarde sont définies au paragraphe 11.

7 Problèmes de sécurité relatifs à l'environnement IaaS

En raison des avantages considérables qu'elles offrent, les infrastructures IaaS sont devenues l'un des services les plus importants des fournisseurs CSP, en particulier pour les opérateurs de télécommunication traditionnels, les fournisseurs OTT (over-the-top) et les fournisseurs de services numériques (DSP); elles sont, de plus, en rapide expansion. Outre le développement rapide des infrastructures IaaS, les questions de sécurité demeurent un sujet de préoccupation majeur dont on ne saurait négliger l'importance. Les plates-formes et services IaaS sont confrontés à davantage de problèmes et de menaces que les infrastructures et applications traditionnelles des technologies de l'information, en particulier en raison de la mise en œuvre à grande échelle des technologies de virtualisation et des ressources partagées pour les multi-locataires, entre autres.

Étant donné qu'une infrastructure IaaS publique peut avoir de nombreux clients CSC qui proviennent de nombreuses organisations différentes et qui coexistent, la sécurité et la protection de la confidentialité sont les facteurs les plus importants lorsque les clients CSC évaluent le choix de services IaaS publics.

En résumé, les problèmes de sécurité auxquels une infrastructure IaaS publique est confrontée peuvent provenir des aspects suivants:

1) Virtualisation: En tant que fonctionnalité technique importante de l'informatique en nuage, la virtualisation permet à plusieurs machines virtuelles (VM) de fonctionner sur le même hyperviseur, mais elle rend également les fichiers contenus dans des machines virtuelles vulnérables au risque d'être modifiés de façon illicite. En outre, lorsque les vulnérabilités de l'hyperviseur sont exploitées, toutes les machines virtuelles qu'il héberge seront soumises aux mêmes risques de sécurité. Ces risques sont causés par:
   - Une configuration et une isolation du réseau inappropriées pour les serveurs physiques. Les auteurs d'attaques peuvent exploiter directement les vulnérabilités de l'hyperviseur.
   - Des vulnérabilités au niveau des interfaces entre les machines virtuelles et l'hyperviseur. Les auteurs d'attaques pourraient exploiter les vulnérabilités afin de prendre le contrôle de l'hyperviseur: c'est ce que l'on appelle une évasion de machine virtuelle.
2) Interfaces API ouvertes: En tant que fondement de la gestion automatique des machines virtuelles, les interfaces API ouvertes sont susceptibles d'offrir une surface vulnérable plus grande par suite de l'utilisation abusive ou de l'exploitation de vulnérabilités liées à l'absence de vérification de l'authentification, des autorisations ou de l'intégrité, ce qui pourrait entraîner la destruction de nombreuses applications.
3) Connectivité réseau et Internet: Les menaces relatives au réseau, telles que les attaques par déni de service réparti (DDoS), les attaques par intercepteur ou les attaques par usurpation d'adresse IP, pourraient être lancées non seulement depuis le réseau traditionnel, mais aussi depuis les machines virtuelles situées sur le même serveur, ce contre quoi il est bien plus difficile de se défendre dans l'environnement d'un réseau virtualisé, dont les frontières sont floues.
4) Niveau élevé de partage des ressources: Cette fonctionnalité technique pourrait constituer une cible de choix. Si le serveur physique ou le réseau physique est détruit, l'ensemble des machines virtuelles qu'il abrite en subiraient les conséquences. L'élimination des dispositifs de stockage vétustes ou des dispositifs de stockage ayant été remplacés a trait à la confidentialité de toutes les données des clients CSC. Ce partage engendrerait en outre des difficultés relatives à l'isolation entre les différents clients CSC. Si l'isolation des différentes machines virtuelles n'est pas configurée correctement, la possibilité de fuite de données ou même d'attaques de réseau entre les différentes machines virtuelles peut considérablement augmenter. Tout incident qui survient peut engendrer des risques et des conséquences importants en matière de sécurité.

5) Évolutivité des ressources virtuelles: L'expansion élastique des ressources virtuelles et l'ajustement dynamique du périmètre de sécurité d'un réseau virtuel entraîne une rapide augmentation du flux de réseau est-ouest ainsi que de nouvelles demandes de sécurité complexes. Les dispositifs de sécurité doivent par conséquent faire preuve d'une certaine agilité et pouvoir fonctionner en collaboration, mais la plupart des équipements et des systèmes de sécurité présentent un fonctionnement individuel. Il leur manque un mécanisme de coopération efficace.

6) Gestion de la configuration: L'environnement de l'informatique en nuage comporte un grand nombre d'installations de plusieurs types ainsi que différents types de services, ce qui entraîne une forte demande en termes de configuration, notamment en ce qui concerne le contrôle d'accès, l'isolation ou encore la sauvegarde des données. Une configuration inadéquate peut donner lieu à une nouvelle surface vulnérable ou même être directement la source d'une fuite d'informations sensibles.

7) Problèmes de journalisation: Les nombreuses données de journaux des systèmes d'exploitation, des applications et des équipements de sécurité peuvent aider les opérateurs à éviter les sinistres par anticipation et même à détecter l'origine des incidents de sécurité. Dans l'environnement de l'informatique en nuage, l'acquisition de données de journaux, la protection et la synchronisation temporelle deviennent plus complexes. Par exemple, l'absence de protection des journaux engendrerait un risque d'altération volontaire et l'absence de synchronisation temporelle rendrait difficile la corrélation de journaux hétérogènes.

8 Exigences de sécurité pour la couche d'accès d'une infrastructure IaaS

La couche d'accès d'une infrastructure IaaS est responsable de la présentation des capacités des services IaaS en matière d'accès et de gestion aux clients CSC. Les mécanismes d'accès comprennent, sans s'y limiter, les éléments suivants:

– Accès web.

– Accès API.

Il revient en outre à la couche d'accès de mettre en œuvre les mécanismes de gestion des connexions appropriés pour garantir l'application des politiques de qualité de service, la répartition de la charge et la transmission sécurisée en ce qui concerne le trafic et les connexions en provenance ou en direction des composantes fonctionnelles de la couche utilisateur.

8.1 Exigences de sécurité pour l'accès web

1) Les fournisseurs CSP d'infrastructures IaaS doivent appliquer les mesures d'authentification et d'autorisation en ce qui concerne l'accès des clients CSC au service IaaS au moyen d'un accès web. Il s'agit par exemple d'authentifier la demande grâce au justificatif d'identité du client CSC et de valider son autorisation.

2) Les fournisseurs CSP d'infrastructures IaaS doivent appliquer un mécanisme de contrôle d'accès pour l'utilisation des capacités de service associées par un client CSC.

3) Il est recommandé que les fournisseurs CSP d'infrastructures IaaS assurent un tunnel de communication sécurisé pour les clients CSC utilisant un accès web.

4) Il est recommandé que les fournisseurs CSP d'infrastructures IaaS garantissent la protection de l'accès web pour les clients CSC, par exemple en procédant à un contrôle de validité à l'entrée et à la sortie, en vérifiant l'intégrité des demandes ou en assurant des capacités de défense contre les comportements d'intrusion web, tels que les injections d'éléments en langage de requête structurée (SQL), les scripts intersites (XSS) ou encore l'exécution de commandes à distance.

5) Les fournisseurs CSP d'infrastructures IaaS doivent prendre en charge des capacités de journalisation sans altération volontaire, d'analyse et d'audit de sécurité pour les comportements d'accès web.

8.2 Exigences de sécurité pour l'accès API

1) Les fournisseurs CSP d'infrastructures IaaS doivent prendre en charge l'authentification et l'authentification du justificatif d'identité de l'utilisateur pour les clients CSC lorsqu'ils font appel à une interface API de service, par exemple lors de la connexion à l'interface API afin de garantir que seules les demandes d'utilisateurs légitimes sont prises en compte.

2) Les fournisseurs CSP d'infrastructures IaaS doivent offrir un mécanisme de contrôle d'accès lorsqu'un client CSC fait appel à l'interface API de service.

3) Il est recommandé que les fournisseurs CSP d'infrastructures IaaS assurent un tunnel de communication sécurisé pour les clients CSC utilisant un accès API.

4) Il est recommandé que les fournisseurs CSP d'infrastructures IaaS garantissent la protection de l'interface API pour les clients CSC, par exemple en vérifiant l'intégrité des demandes ou en assurant des capacités de défense contre les comportements d'attaque, tels que les attaques par réexécution ou encore les injections de code.

5) Les fournisseurs CSP d'infrastructures IaaS doivent prendre en charge des capacités de journalisation, d'analyse et d'audit de sécurité pour les comportements d'accès API.

9 Exigences de sécurité pour la couche service d'une infrastructure IaaS

La couche service d'une infrastructure IaaS comprend la mise en œuvre des services assurés par le fournisseur CSP. La couche service comprend et commande les composantes logicielles qui mettent en œuvre les services IaaS (tels que le service de calcul, le service de réseau, le service de stockage, etc.) et permet de mettre ces services IaaS à la disposition des clients CSC au moyen de la couche d'accès.

9.1 Exigences de sécurité pour le service de calcul

1) Les fournisseurs CSP d'infrastructures IaaS doivent assurer des mécanismes d'isolation pour les ressources virtuelles, y compris l'isolation de l'unité de traitement centrale (CPU), des réseaux internes, de la mémoire ou encore du stockage et doivent autoriser uniquement les communications qui sont conformes aux politiques de sécurité entre les différentes unités de ressource virtuelle, telles que les machines virtuelles.

2) Les fournisseurs CSP d'infrastructures IaaS doivent prendre en charge le réglage de la limite supérieure des ressources disponibles pour une seule unité de ressource virtuelle au sein d'un serveur physique, ce qui permet d'éviter la dégradation des performances en raison d'une occupation excessive d'une unité de ressource virtuelle particulière.

3) Il est recommandé que les fournisseurs CSP d'infrastructures IaaS prennent en charge la migration automatique de l'unité de ressource virtuelle en cas de défaillance au niveau du serveur hébergé, ce qui pourrait éviter l'interruption des services exécutés sur la ressource virtuelle.

4) Les fournisseurs CSP d'infrastructures IaaS doivent prendre en charge la vérification de l'intégrité des images de l'unité de ressource virtuelle, afin d'éviter les altérations malveillantes, et garantir qu'un volume logique ne soit utilisé que par une unité de ressource virtuelle à la fois.

5) Les fournisseurs CSP d'infrastructures IaaS doivent prendre en charge la migration des politiques de sécurité, qui seraient alors synchronisées simultanément avec l'unité de ressource virtuelle.

6) Les fournisseurs CSP d'infrastructures IaaS doivent fournir à l'administrateur du client CSC la possibilité d'adapter les politiques de sécurité suivant les différentes unités de ressource virtuelle.

7) Les fournisseurs CSP d'infrastructures IaaS doivent fournir aux clients CSC la possibilité de supprimer la totalité de leurs données personnelles. Lorsqu'une unité de ressource virtuelle est supprimée par le client CSC, les fichiers d'image, les instantanés et les sauvegardes doivent aussi être supprimés de façon immédiate.

9.2 Exigences de sécurité pour le service de stockage

1) Il est recommandé que les fournisseurs CSP d'infrastructures IaaS prennent en charge un mécanisme de redondance des données. Les données des clients CSC devraient faire l'objet d'un minimum de deux sauvegardes situées en des emplacements physiques différents et ce mécanisme doit être transparent vis-à-vis des clients CSC.

2) Il est recommandé que les fournisseurs CSP d'infrastructures IaaS prennent en charge les commandes d'entrée/sortie (I/O) simultanées et l'accès sécurisé en parallèle par plusieurs machines virtuelles qui utilisent le même système de stockage.

3) Les fournisseurs CSP d'infrastructures IaaS doivent garantir le contrôle d'accès aux données stockées, qui peut être exécuté à la fois sur les entités de stockage logiques et physiques et qui ne doit pas être contourné par une quelconque modification de l'emplacement physique de stockage.

4) Les fournisseurs CSP d'infrastructures IaaS doivent garantir que les données des clients CSC puissent être entièrement supprimées:

   − La suppression complète des données doit être réalisée avant que la ressource de stockage ne soit attribuée à un nouveau client CSC.

   − Lorsque des fichiers ou l'objet d'un client CSC sont supprimés, la zone de stockage correspondante dans le volume physique doit être correctement écrasée ou être étiquetée comme en écriture seulement, évitant ainsi une récupération non autorisée des informations.

   − Lorsque les données d'un client CSC sont déplacées, toutes les métadonnées du client CSC doivent être immédiatement supprimées.

9.3 Exigences de sécurité pour le service de réseau

1) Il est recommandé que les fournisseurs CSP d'infrastructures IaaS fournissent aux clients CSC la possibilité de surveiller le trafic nord-sud et est-ouest de leurs propres ressources virtuelles.

2) Il est recommandé que les fournisseurs CSP d'infrastructures IaaS fournissent aux clients CSC la possibilité de mettre en œuvre le contrôle de la largeur de bande des ressources virtuelles à l'interface de réseau.

3) Les fournisseurs CSP d'infrastructures IaaS doivent appliquer des mesures d'isolation entre le réseau virtualisé des clients CSC et la plate-forme IaaS et le réseau de gestion, par exemple en interdisant l'accès des clients CSC au serveur ou au nœud de gestion.

4) Les fournisseurs CSP d'infrastructures IaaS doivent mettre en œuvre un mécanisme de liste de contrôle d'accès (ACL) au réseau, afin de garantir l'isolation relative à la sécurité et le contrôle d'accès pour les réseaux virtualisés.

5) Il est recommandé que les fournisseurs CSP d'infrastructures IaaS prennent en charge la défense contre les attaques de réseau, notamment les attaques par saut de réseau local virtuel (VLAN) ou de réseau local extensible virtuel (VXLAN).

10 Exigences de sécurité pour la couche ressources d'une infrastructure IaaS

Compte tenu des composantes fonctionnelles de la couche ressources d'une infrastructure IaaS, les exigences de sécurité pour cette couche comprennent:

– des exigences de sécurité pour la représentation abstraite et le contrôle des ressources; et

– des exigences de sécurité pour les ressources physiques.

10.1 Exigences de sécurité pour la représentation abstraite et le contrôle des ressources

La composante fonctionnelle relative à la représentation abstraite et au contrôle des ressources permet aux fournisseurs CSP d'offrir des caractéristiques telles qu'une élasticité rapide, la mutualisation des ressources et un libre-service à la demande. Le pool de ressources virtuelles (par exemple les ressources de calcul virtuelles, les ressources de réseau virtuelles, etc.) et la plate-forme de gestion des ressources virtuelles font partie de cette composante. Les exigences de sécurité pour la représentation abstraite et le contrôle des ressources seront considérées du point de vue de la fourniture et de la gestion des ressources virtuelles.

10.1.1 Exigences de sécurité pour le pool de ressources virtuelles

10.1.1.1 Exigences de sécurité pour les ressources de calcul virtuelles

1) Les unités de ressource de calcul virtuelle (par exemple une machine virtuelle, un conteneur, etc.) doivent être isolées logiquement les unes des autres.

2) Il est nécessaire que l'unité de ressource de calcul virtuelle ne puisse pas être influencée par d'autres unités ou d'autres serveurs en cas de défaillance ou d'incidents anormaux.

3) Il est nécessaire que l'unité de ressource de calcul virtuelle ne puisse pas être utilisée au-delà du quota qui lui est attribué.

4) Il est recommandé que les fonctions "copier", "coller" ainsi que d'autres commandes soient interdites entre différentes unités de ressource de calcul virtuelle ou différents serveurs.

5) Il est recommandé que les fournisseurs CSP d'infrastructures IaaS prennent en charge la surveillance en temps réel des ressources virtuelles au moyen d'un mode dans la bande ou hors bande, et que des alarmes soient envoyées lorsque des anomalies sont détectées. Pour chaque unité de ressource virtuelle, les objets surveillés doivent notamment comprendre l'état de fonctionnement, la consommation de ressources et le statut de migration.

10.1.1.2 Exigences de sécurité pour les ressources de réseau virtuelles

1) Les réseaux virtuels des clients CSC doivent être isolés logiquement les uns des autres par la mise en œuvre des mesures des réseaux VLAN, VXLAN, des listes ACL, etc.

2) Une capacité de surveillance du trafic du réseau doit être assurée entre les différentes unités de ressource virtuelle.

3) Une capacité de contrôle du débit doit être assurée au niveau des ports virtuels.

4) Il est recommandé que les comportements d'attaque de réseau (par exemple, l'usurpation d'adresse IP, des vers, etc.) émanant des ressources virtuelles puissent être détectés et contrecarrés.

5) Le mode promiscuité des ports virtuels de la carte d'interface de réseau (NIC) doit être interdit afin d'empêcher le reniflage du trafic du réseau.

10.1.1.3 Exigences de sécurité pour les ressources de stockage virtuelles

1) Le pool de ressources de stockage virtuelles doit être isolé entre les différents clients CSC.

2) Les mesures de sécurité portant sur les données stockées doivent être exécutées à la fois sur les entités de stockage logiques et physiques.

3) L'accès direct aux ressources de stockage physiques doit être interdit.

4) La capacité de commandes d'entrée/sortie (I/O) simultanées et d'accès sécurisé en parallèle doit être prise en charge pour les différentes unités de ressource virtuelle qui utilisent les mêmes entités de stockage.

5) Il est recommandé que les ressources de stockage virtuelles puissent prendre en charge une expansion élastique sans interruption des services de stockage normaux.

10.1.2 Exigences de sécurité pour les plates-formes de gestion des ressources virtuelles

1) Les mesures de contrôle d'accès doivent être mises en œuvre de manière appropriée afin d'empêcher un accès illégal à la plate-forme de gestion des ressources virtuelles.

2) Il est recommandé que seules les composants et applications nécessaires soient installés et que les ports de service inappropriés soient fermés, dans le cadre du respect du principe de réduction des risques.

3) Il est nécessaire que les comportements d'attaque visant la plate-forme de gestion des ressources virtuelles puissent être détectés et qu'une alarme soit envoyée en temps voulu; les journaux devraient être enregistrés, y compris l'adresse IP source, le type d'attaque, l'horodate, etc.

4) La capacité de surveillance en temps réel des ressources virtuelles doit être assurée; elle comprend notamment l'état de fonctionnement, l'occupation des ressources et la migration.

5) Il est recommandé que les ressources virtuelles inutiles et libres puissent être désactivées.

6) Les commandes de gestion effectuées au moyen d'une plate-forme de gestion des ressources virtuelles doivent être transmises dans un tunnel sécurisé.

7) Il est recommandé que les commandes privilégiées puissent être restreintes lorsqu'elles sont exécutées à distance.

8) Il est nécessaire que les unités de ressource virtuelle illicites puissent être isolées et éliminées de manière appropriée, afin de réduire les effets induits sur la totalité des ressources virtuelles.

9) La capacité de détection et d'élimination de code malveillant doit être assurée.

10) Il est recommandé que les politiques de sécurité puissent être migrées conjointement avec la migration simultanée des unités de ressource virtuelle.

11) Les correctifs de sécurité ou les configurations visant à renforcer la sécurité doivent être mis en œuvre en temps voulu lorsque des vulnérabilités liées à la sécurité sont détectées dans les composantes de gestion des ressources virtuelles (par exemple un hyperviseur, un moteur de conteneurs, les composantes de gestion, etc.); ils doivent en outre être tenus à jour.

12) La gestion des défaillances doit être assurée afin de garantir la continuité des services supérieurs; autrement dit, les unités de ressource virtuelle situées sur un serveur défaillant peuvent être migrées en temps voulu vers un autre serveur.

13) Toutes les opérations et tous les événements relatifs à la plate-forme de gestion des ressources virtuelles doivent être journalisés à des fins de traçabilité et d'audit ultérieurs.

10.2 Exigences de sécurité pour les ressources physiques

Les ressources physiques comprennent les ressources matérielles, telles que les ordinateurs, les équipements de réseau, les composants de stockage ainsi que d'autres éléments de l'infrastructure informatique physique, nécessaires pour que le fournisseur CSP puisse exécuter et gérer les services IaaS offerts aux clients CSC.

10.2.1 Exigences de sécurité pour l'environnement physique

Les exigences de sécurité pour l'environnement physique d'une infrastructure IaaS figurent dans la norme [ISO/CEI 27002].

10.2.1.1 Exigences de sécurité pour les ressources physiques

Les ressources physiques comprennent les ressources matérielles, telles que l'infrastructure de réseau physique, les dispositifs de stockage, les serveurs, les terminaux de gestion et d'autres éléments de l'infrastructure physique.

1) La capacité de détection des défaillances et de leur emplacement dans les ressources physiques (par exemple, les équipements de réseau, les serveurs, les dispositifs de stockage, etc.) doit être assurée afin de garantir la disponibilité et la fiabilité de l'infrastructure physique sous-jacente.
2) Il est recommandé que l'altération des ressources physiques puisse être détectée et marquée en temps voulu.
3) Il est recommandé que la capacité de récupération des données puisse être assurée lorsque des composants physiques subissent des défaillances.
4) La capacité de défense de la plate-forme IaaS contre les attaques DDoS doit être assurée.
5) Le réseau d'infrastructure doit être divisé en différents domaines de sécurité du réseau, isolés logiquement les uns des autres.
6) Les mécanismes de détection des comportements de surveillance du trafic du réseau et d'intrusion doivent être mis en œuvre, au moyen de dispositifs de protection déployés aux frontières du réseau, notamment la gestion des identités et de l'accès (IAM), un système IPS, un pare-feu, etc.
7) Il est recommandé que les comportements d'attaque de réseau sortants qui proviennent des ressources IaaS puissent être détectés et contrecarrés.
8) Une capacité de détection et d'élimination de code malveillant doit être assurée, en particulier pour les terminaux de gestion, les serveurs et d'autres serveurs d'application.
9) Il est nécessaire que les politiques de sécurité de base soient mises en œuvre et que seuls les terminaux et les serveurs qui répondent aux politiques de sécurité puissent accéder à la plate-forme IaaS.
10) Toutes les opérations et tous les événements relatifs aux ressources physiques doivent être journalisés à des fins de traçabilité et d'audit ultérieurs.

11 Exigences relatives à la gestion de la sécurité

La gestion de la sécurité est responsable de l'application des contrôles relatifs à la sécurité, afin de réduire les menaces de sécurité dans les environnements de l'informatique en nuage. Les composantes fonctionnelles de la gestion de la sécurité comprennent tous les dispositifs de sécurité nécessaires pour la prise en charge des services en nuage.

Les composantes fonctionnelles de la gestion de la sécurité comprennent:

- la gestion des identités et le contrôle d'accès;
- l'audit de sécurité;
- la gestion des vulnérabilités;
- l'intervention en cas d'urgence;
- la reprise après sinistre; et
- la sauvegarde.

11.1 Gestion IdM et contrôle d'accès

Une plate-forme IaaS devrait fournir des fonctions unifiées de gestion des identités (IdM) et de contrôle d'accès aux clients CSC et aux administrateurs de la plate-forme IaaS.

1) L'identité d'un client CSC au cours du cycle de vie doit être unique dans chaque service IaaS et associée à un audit de sécurité. L'identité d'un client CSC doit être gérée, maintenue et protégée contre les accès, les modifications et les suppressions non autorisés.

2) Une plate-forme IaaS doit assurer la gestion des politiques relatives aux mots de passe pour les clients CSC, comprenant, sans s'y limiter:
   - la nécessité d'appliquer des politiques relatives à la complexité des mots de passe;
   - la nécessité d'appliquer un mécanisme de redéfinition périodique des mots de passe;
   - la nécessité d'utiliser une clé initiale générée de manière aléatoire pour les clients CSC, devant être modifiée lors de la première connexion.

3) Il est recommandé que les plates-formes IaaS prennent en charge la détection des anomalies pour les identités des clients CSC et que des alarmes soient envoyées aux clients CSC concernés.

4) Les plates-formes IaaS doivent prendre en charge l'authentification à plusieurs facteurs pour les clients CSC ainsi que des techniques d'authentification comprenant, sans s'y limiter, les mots de passe, les certificats numériques, les cartes IC ou la validation biométrique.

5) Il est nécessaire que la stratégie d'autorisation à granularité fine soit prise en charge, en fonction du client CSC et de la définition de groupe des ressources auxquelles l'accès est demandé. Il est nécessaire que la plate-forme IaaS protège la confidentialité et l'intégrité des justificatifs d'authentification des clients CSC.

6) Les journaux détaillés de l'authentification, de l'autorisation et d'autres opérations des clients CSC relatives à la gestion IdM doivent être stockés à des fins d'audit ultérieur.

7) Il est recommandé que les plates-formes IaaS prennent en charge la connexion avec les systèmes IdM des clients CSC.

8) Le rôle et les privilèges associés de l'administrateur d'une plate-forme IaaS doivent être accordés à différents comptes.

9) Les plates-formes IaaS doivent utiliser l'authentification à plusieurs facteurs pour les administrateurs.

10) Les plates-formes IaaS doivent appliquer le principe d'autorité minimale pour les administrateurs.

11) Les données sensibles telles que les données d'authentification ou encore les données d'autorisation doivent être chiffrées lors de la procédure de stockage et de transfert.

11.2 Audit de sécurité

1) Les plates-formes IaaS doivent utiliser divers journaux pour les audits de sécurité, comprenant, sans toutefois s'y limiter:
   - la journalisation, les informations d'authentification et d'autorisation des identités des clients CSC et des administrateurs de la plate-forme IaaS;
   - l'exploitation et la tenue à jour de journaux concernant l'infrastructure IaaS par les administrateurs de la plate-forme IaaS;
   - l'exploitation de journaux concernant les ressources des clients CSC par les administrateurs de la plate-forme IaaS;

– l'exploitation de journaux concernant les ressources propres aux clients CSC par les clients CSC;
– l'exploitation et la tenue à jour de journaux lors de l'exécution de processus de la plate-forme IaaS.

2) Les plates-formes IaaS doivent mettre en œuvre des mécanismes de sécurité visant à protéger les différents journaux contre les altérations volontaires.

3) Toutes les horloges du réseau doivent être synchronisées en permanence dans l'ensemble de la plate-forme IaaS, afin de permettre l'enregistrement des accès et des opérations de manière systématique.

4) Les journaux d'audit de sécurité doivent comprendre les sujets, les objets, l'heure et la date, le type et les résultats des événements liés à la sécurité.

5) Les journaux d'audit entre les clients CSC doivent être isolés les uns des autres.

6) Il est nécessaire que les clients CSC puissent obtenir et consulter les journaux d'audit concernant leurs propres ressources.

7) Les journaux d'audit doivent être solidement protégés, par exemple en interdisant les accès non autorisés aux journaux d'audit, en empêchant les suppressions, modifications, remplacements et pertes imprévus.

8) La période de conservation des journaux d'audit doit être conforme aux exigences légales ainsi qu'aux exigences particulières des clients CSC.

9) Il est recommandé que les plates-formes IaaS puissent permettre aux clients CSC d'utiliser des systèmes ou une interface d'audit tiers, afin d'atteindre les objectifs d'audit s'inscrivant dans le cadre des responsabilités des clients CSC.

11.3 Gestion des vulnérabilités

Les vulnérabilités d'une plate-forme IaaS peuvent concerner les processus, la gestion, la configuration, le matériel, les logiciels, etc.

1) Il est nécessaire de tenir un journal des informations concernant tous les dispositifs ainsi que les versions de la plate-forme IaaS, et de mettre à jour ces informations régulièrement.

2) Il est nécessaire de mettre au point un mécanisme d'évaluation des vulnérabilités, dans lequel les objets, la fréquence et la stratégie d'évaluation des vulnérabilités devraient être clairement définis.

3) Il est nécessaire de réaliser régulièrement une évaluation des vulnérabilités sur tous les dispositifs d'une plate-forme IaaS, de générer des rapports d'évaluation des vulnérabilités et de formuler des recommandations pour les corriger.

4) Il est nécessaire que des processus de correctif et de réparation soient mis en œuvre:
   − Il est nécessaire d'assurer un suivi des menaces de sécurité et des correctifs de sécurité distribués par les différents vendeurs et de déterminer quels correctifs doivent être installés sur la plate-forme IaaS.
   − Il est nécessaire de tester les correctifs de sécurité avant l'installation, afin de s'assurer qu'ils sont compatibles avec les systèmes et applications existants.
   − Il est nécessaire de créer le plan de mise à jour des correctifs pour tous les composants de la plate-forme IaaS, de réaliser l'installation des correctifs conformément à ce plan et de créer des journaux au cours de l'installation.

5) Il est nécessaire de définir la configuration de sécurité de base de la plate-forme IaaS et de configurer les composantes de la plate-forme IaaS en conséquence.

6) Il est nécessaire d'inspecter régulièrement tous les dispositifs de la plate-forme IaaS en termes de sécurité de base, d'établir un rapport d'inspection correspondant et de formuler des recommandations pour corriger les manquements.

7) Il est nécessaire de réaliser des audits concernant les modifications des stratégies de configuration de la plate-forme IaaS, afin de vérifier que chaque paramètre de configuration est correct, cohérent, complet et efficace ainsi que pour garantir que les modifications de la configuration n'engendrent pas de nouveaux défauts de sécurité.

11.4 Intervention en cas d'urgence

Les considérations relatives à l'intervention en cas d'urgence pour les infrastructures IaaS sont conformes au § 8.9 de la Recommandation [UIT-T X.1642].

11.5 Reprise après sinistre

Les considérations relatives à la reprise après sinistre des infrastructures IaaS devraient être conformes aux réglementations communes existantes concernant les technologies de l'information, par exemple la norme [ISO/CEI 27031]. Cependant, en raison de la croissance rapide de cette technologie, la reprise après sinistre des infrastructures IaaS doit aussi tenir compte des éléments suivants:

1) Définition des objets de reprise après sinistre pour chaque client CSC. Il est nécessaire de réaliser une analyse d'impact sur les activités (BIA) afin de déterminer les objets de reprise après sinistre des différentes activités, en fonction de la reconnaissance des composantes clés et des principaux risques de sécurité de la plate-forme IaaS. Les objets de reprise après sinistre peuvent être définis en termes de priorités, d'objectifs RPO/RTO, etc. Les différents objets DRO déterminent l'accord SLA correspondant et l'architecture des services, notamment les technologies à grande disponibilité entre les centres de données virtuels (VDC), les sauvegardes de données interrégionales, etc.

2) Sauvegarde régulière des systèmes et des données. Il est nécessaire de prendre en charge la capacité de stockage de données interrégional et de résistance aux sinistres. En outre, les types de sauvegardes au niveau du système et au niveau des données devraient être fournis aux locataires de la plate-forme IaaS, de même que la capacité de reprise après sinistre correspondante, ce qui peut aider les fournisseurs CSP et les clients CSC à mettre en œuvre la reprise après défaillance. En ce qui concerne les clients CSC, ils peuvent en outre sauvegarder régulièrement les données auprès d'un fournisseur CSP différent, afin d'éviter le risque d'interruption pendant une longue période représenté par un seul fournisseur CSP.

3) Validation régulière du plan de reprise après sinistre. Bien que les systèmes et les données des clients CSC demeurent relativement constants, de nouveaux risques de sécurité peuvent être engendrés par des mises à jour de l'infrastructure effectuées par les fournisseurs CSP. Par conséquent, des exercices de reprise après sinistre devraient être réalisés régulièrement et les informations clés devraient être enregistrées, notamment celles concernant la disponibilité, l'intégrité et la validité des plans de reprise après sinistre, ainsi que les problèmes survenus lors du processus et les solutions correspondantes.

4) Évaluation régulière des risques. Pour garantir la continuité des activités des clients CSC, les fournisseurs CSP devraient évaluer les risques de sécurité pouvant avoir des incidences sur le plan de continuité des activités des clients CSC, ce qui comprend les défaillances des services IaaS, les interruptions du réseau entre les fournisseurs CSP et les clients CSC, la cessation des services en nuage, etc., et les résultats devraient être dûment transmis aux clients CSC. En outre, l'intervention en cas d'urgence, les plans de reprise après sinistre et les mesures visant à assurer la continuité des activités des clients CSC devraient être indiqués en amont et adaptés en fonction des exigences des clients CSC.

11.6 Sauvegarde

Les considérations relatives à la sauvegarde pour les infrastructures IaaS sont conformes au § 8.10 de la Recommandation [UIT-T X.1642].

Bibliographie

[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-NIST 500-291] Publication spéciale du NIST 500-291, 2011, *NIST Cloud Computing Standards Roadmap*.

[b-NIST-SP-800-30] Publication spéciale du NIST 800-30, 2012, *Guide for Conducting Risk Assessments*.

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, 2020