ITUPublications
Recommandations

Union internationale des télécommunications
Secteur de la normalisation

Recommandation

UIT-T X.1644 (03/2023)

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 du nuage réparti

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 (1)	X.1140–X.1149
Sécurité des applications (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.1350–X.1369
Sécurité des systèmes de transport intelligents	X.1370–X.1399
Sécurité de la technologie des registres distribués (DLT)	X.1400–X.1429
Sécurité des applications (2)	X.1450–X.1459
Sécurité de la toile (2)	X.1470–X.1489
ÉCHANGE D'INFORMATIONS SUR LA CYBERSÉCURITÉ	
Aperçu général de la cybersécurité	X.1500–X.1519
Échange concernant les vulnérabilités/les états	X.1520–X.1539
Échange concernant les événements/les incidents/l'heuristique	X.1540–X.1549
Échange de politiques	X.1550–X.1559
Heuristique et demande d'informations	X.1560–X.1569
Identification et découverte	X.1570–X.1579
Échange garanti	X.1580–X.1589
Cyberdéfense	X.1590–X.1599
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 œuvre de la sécurité de l'informatique en nuage	X.1660–X.1679
Sécurité de l'informatique en nuage (autres)	X.1680–X.1699
COMMUNICATIONS QUANTIQUES	
Terminologie	X.1700–X.1701
Générateur quantique de nombres aléatoires	X.1702–X.1709
Cadre de sécurité pour les réseaux QKDN	X.1710–X.1711
Conception de la sécurité pour les réseaux QKDN	X.1712–X.1719
Techniques de sécurité pour les réseaux QKDN	X.1720–X.1729
SÉCURITÉ DES DONNÉES	
Sécurité des mégadonnées	X.1750–X.1759
Protection des données	X.1770–X.1789
SÉCURITÉ DES IMT-2020	X.1800–X.1819

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

Recommandation UIT-T X.1644

Lignes directrices relatives à la sécurité du nuage réparti

Résumé

La Recommandation UIT-T X.1644 contient une analyse des menaces et des problèmes de sécurité concernant le nuage réparti, et vise à proposer des lignes directrices relatives à la sécurité afin de lutter contre les menaces visant le nuage réparti, y compris des lignes directrices relatives à la sécurité du nuage central, du nuage régional et du nuage en périphérie.

Historique

Edition	Recommandation	Approbation	Commission d'études	ID Unique *
1.0	UIT-T X.1644	03-03-2023	17	11.1002/1000/15112

Mots clés

Informatique en nuage, nuage réparti, lignes directrices relatives à la sécurité

* 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 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.

À 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 ou par des droits d'auteur afférents à des logiciels, et dont l'acquisition pourrait être requise 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 responsables de la mise en œuvre de consulter les bases de données appropriées de l'UIT-T disponibles sur le site web de l'UIT-T à l'adresse http://www.itu.int/ITU-T/ipr/.

TABLE DES MATIÈRES

Recommandation UIT-T X.1644

Lignes directrices relatives à la sécurité du nuage réparti

1 Domaine d'application

La présente Recommandation contient une analyse des menaces de sécurité concernant le nuage réparti et vise à fournir des lignes directrices relatives à la sécurité du nuage réparti.

2 Références

Les Recommandations UIT-T et autres références suivantes contiennent des dispositions qui, par suite de la référence qui y est faite, constituent des dispositions de la présente Recommandation. Au moment de la publication, les éditions indiquées étaient en vigueur. Toutes les Recommandations et autres références étant sujettes à révision, les utilisateurs de la présente Recommandation sont invités à se reporter, si possible, aux versions 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 d'une Recommandation.

[UIT-T X.1408] Recommandation UIT-T X1408 (2021), *Menaces et exigences de sécurité relatives à l'accès aux données et au partage de données reposant sur la technologie des registres distribués.*

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

[UIT-T Y.3500] Recommandation UIT-T Y.3500 (2014), *Technologies de l'information – Informatique en nuage – Présentation générale et vocabulaire.*

[UIT-T Y.3508] Recommandation UIT-T Y.3508 (2019), *Informatique en nuage répartie: aperçu et exigences de haut niveau.*

3 Définitions

3.1 Termes définis ailleurs

La présente Recommandation utilise les termes suivants définis ailleurs:

3.1.1 type de capacités de nuage [UIT-T Y.3500]: classification de la fonctionnalité fournie par un service en nuage au client de services en nuage (CSC), en fonction des ressources utilisées.

NOTE – Les types de capacités de nuage sont les suivants: capacités de type application, capacités de type infrastructure et capacités de type plate-forme.

3.1.2 informatique en nuage [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.

3.1.3 service en nuage [UIT-T Y.3500]: une ou plusieurs capacités offertes via l'informatique en nuage invoquées à l'aide d'une interface définie.

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

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

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

3.1.6 nuage en périphérie [UIT-T Y.3508]: informatique en nuage déployée à la périphérie du réseau à laquelle accèdent des clients de services en nuage (CSC) ayant des ressources de faible capacité.

NOTE 1 – Les services en nuage fondés sur le nuage en périphérie sont des services légers fournis par un fournisseur de services en nuage (CSP) selon la catégorie de services en nuage.

NOTE 2 – Les services en nuage légers correspondent à une portion de services en nuage destinée à reconfigurer la fonctionnalité des services en nuage de façon à convenir au nuage en périphérie, comme les stations de base et les passerelles avec des ressources de faible capacité.

3.1.7 menace [UIT-T X.1408]: cause potentielle d'un incident indésirable, susceptible de nuire à un système ou à une organisation.

3.2 Termes définis dans la présente Recommandation

La présente Recommandation définit les termes suivants:

3.2.1 nuage central: ensemble centralisé de services comprenant tous les services indépendants de la situation géographique, les services qui ne sont pas sensibles au temps de latence, les services fortement consommateurs de ressources informatiques, les services de sauvegarde et de rétablissement, et les services à haut niveau de sécurité d'un réseau d'informatique en nuage.

3.2.2 nuage réparti: extension des concepts traditionnels d'informatique en nuage, qui étend les capacités de l'informatique en nuage au-delà de la périphérie du réseau.

3.2.3 nuage régional: nuage central déployé de manière optionnelle pour une configuration efficace entre le nuage central et le nuage en périphérie afin de réduire la charge sur le nuage central.

4 Abréviations et acronymes

La présente Recommandation utilise les abréviations et acronymes suivants:

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

CC nuage central (*core cloud*)

CSC consommateur de service en nuage *(cloud service customer)*

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

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

DoS déni de service *(denial of service)*

EC nuage en périphérie (*edge cloud*)

IoT Internet des objets *(Internet of things)*

OTA transmission sans fil (over-the-air)

REST transfert d'état représentationnel *(representational state transfer)*

TLS sécurité de la couche transport *(transport layer security)*

VPN réseau privé virtuel *(virtual private network)*

XML langage de balisage extensible *(extensible markup language)*

XSS exécution de script intersites *(cross site scripting)*

5 Conventions

Dans la présente Recommandation:

L'expression "**il est obligatoire**" 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.

6 Aperçu

L'informatique en nuage répartie est en plein essor car de plus en plus de services sensibles au temps de latence (comme les services vidéo et les services de l'Internet des objets (IoT)) nécessitent des délais de réponse beaucoup plus rapides. Il s'agit d'une extension de l'informatique en nuage classique qui étend ses capacités au-delà de la périphérie du réseau. Elle peut fournir des services en nuage localisés beaucoup plus proches du client ainsi que des sources de données, et peut interagir avec d'autres plates-formes en nuage pour fournir des services répartis, à faible temps de latence et de haut niveau.

L'informatique en nuage répartie comprend la distribution de types de capacités de nuage à la périphérie du réseau afin de permettre la fourniture de services en nuage caractérisés par un faible temps de latence et un traitement en temps réel, sur une largeur de bande limitée, par interfonctionnement avec un ensemble de ressources physiques et de ressources virtuelles [UIT-T Y.3508]. La Figure 6-1 illustre un exemple type de nuage réparti, comprenant également le nuage central, le nuage régional et le nuage en périphérie.

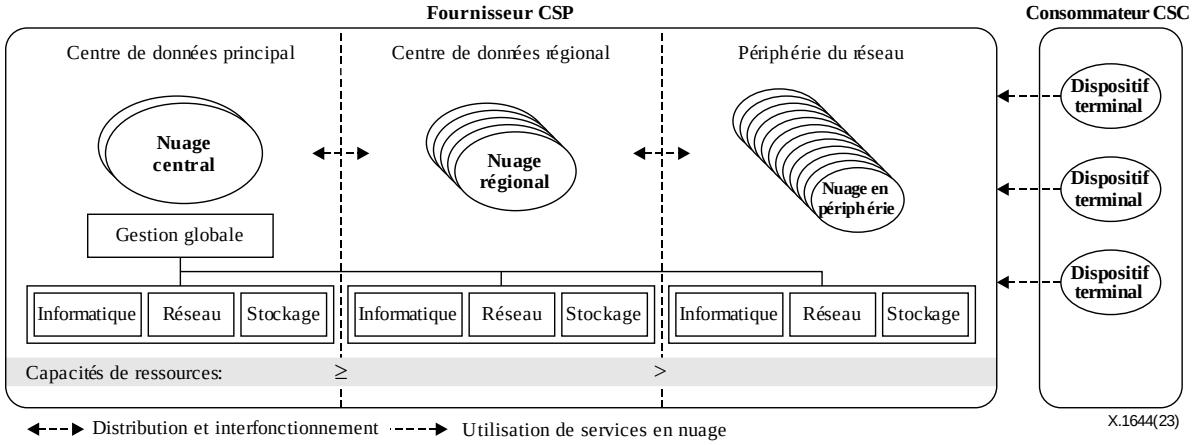

Figure 6-1 – Concept de nuage réparti

Le nuage central est doté d'une grande capacité de ressources et d'un point de gestion central permettant de contrôler les ressources en nuage dans le nuage réparti. Le nuage central prend en charge les services en nuage caractérisés par une intensité informatique élevée et une forte indépendance géographique.

Le nuage régional est déployé de manière optionnelle dans des régions données, depuis le nuage central, afin de partager la charge et d'améliorer la qualité de service. Le nuage régional traite les demandes de services en nuage émanant de la région sous contrôle grâce à la gestion globale du nuage central.

NOTE 1 – Le nuage régional prend en charge des temps de latence inférieurs par rapport au nuage central, en exécutant des services en nuage personnalisés pour les consommateurs CSC dans une région donnée. Il est admis que le temps de latence du consommateur CSC au nuage régional est inférieur à celui du consommateur CSC au nuage central, et que la différence de temps d'exécution entre le nuage central et le nuage régional est négligeable.

NOTE 2 – Le nuage régional assure la mise en mémoire tampon pour la charge du service en nuage et la mise en cache des données à partir du nuage central, et les fournit aux consommateurs CSC dans la région.

Le nuage en périphérie est déployé à la périphérie du réseau auquel les consommateurs CSC accèdent, et dispose d'une faible capacité de ressources. Le nuage en périphérie nécessite expressément des ressources matérielles spécialisées; en effet, les ressources dans le nuage en périphérie sont limitées en raison du manque d'espace ou de puissance. Le nuage en périphérie peut comporter différentes configurations de ressources et différents types de capacités de nuage, avec des ressources physiques et des ressources virtuelles en fonction des exigences d'un consommateur CSC et des conditions en vigueur dans l'environnement de déploiement.

7 Problèmes et menaces de sécurité pour le nuage réparti

L'utilisation d'un nuage réparti offre des avantages s'agissant du haut débit, de l'efficacité et de la qualité de fonctionnement. Le nuage central, le nuage régional et le nuage en périphérie dans un contexte de nuage réparti apportent leur lot de menaces et de problèmes inédits en matière de sécurité [UIT-T X.1601].

7.1 Problèmes et menaces de sécurité pour le nuage central

Le nuage réparti possède des infrastructures de différentes échelles, avec une grande capacité de ressources dans le nuage central ou régional et une faible capacité de ressources dans le nuage en périphérie. Le nuage central utilise une infrastructure hétérogène en tant que système unique pour fournir une gamme de services aux consommateurs CSC dans le nuage réparti. Les problèmes et les menaces de sécurité pour le nuage central sont les suivants:

a) **Vulnérabilités du système**: L'infrastructure en nuage réparti contient des vulnérabilités du système, en particulier dans les réseaux qui possèdent des infrastructures complexes et plusieurs plates-formes tierces, et une vulnérabilité dans le nuage central a aussi des répercussions sur le nuage régional et le nuage en périphérie.

b) **Dommages matériels**: L'infrastructure en nuage réparti peut être déployée dans des environnements matériels non sécurisés et subir des dommages matériels causés par des utilisateurs malveillants, de mauvaises conditions météorologiques ou des tremblements de terre. Des dommages matériels du nuage central peuvent aussi influer sur la sécurité du nuage régional et du nuage en périphérie.

7.2 Problèmes et menaces de sécurité pour le nuage régional

a) **Interception des transmissions**: Le nuage central doit transmettre les données avec les nuages régionaux et il se peut que les liaisons de transmission soient interceptées.

b) **Ordre ou demande provenant d'un dispositif de contrefaçon**: Un ordre ou une demande malveillant(e) provenant d'un nuage central, régional ou en périphérie d'un dispositif de contrefaçon peut entraîner des fuites de données.

c) **Attaque d'interfaces**: Étant donné qu'un nuage central est relié à plusieurs nuages régionaux via des interfaces ouvertes, il se peut que ce nuage soit attaqué par le biais de ces interfaces.

d) **Attaque du puits (*sinkhole*)**: Un intrus peut compromettre un dispositif ou introduire un dispositif de contrefaçon dans le réseau et l'utiliser pour lancer une attaque du puits. Il s'agit d'une forme d'attaque de la couche réseau dans laquelle un dispositif compromis envoie de fausses informations de routage à une entité voisine pour attirer à lui le trafic de réseau.

e) **Passerelles malveillantes**: Il est facile pour l'auteur d'une attaque de déployer une passerelle malveillante. Dès qu'un dispositif légitime est trompé et se connecte à une passerelle malveillante, il est possible de rassembler des informations confidentielles sur les connexions, contournant ainsi, dans la pratique, nombre des mesures de sécurité en place et risquant même de causer des brouillages radioélectriques à l'installation officielle de l'organisation.

f) **Accès non autorisé aux passerelles IoT**: L'auteur d'une attaque peut utiliser un accès non autorisé aux passerelles IoT, ce qui peut entraîner la divulgation d'informations sensibles, la modification de données et l'utilisation illicite de certaines ressources dans le nuage en périphérie.

7.3 Problèmes et menaces de sécurité pour le nuage en périphérie

a) **Problèmes multilocataires**: De nombreuses solutions en nuage ne garantissent pas la protection de la sécurité nécessaire entre les clients, ce qui entraîne le partage des ressources, des applications et des systèmes. Dans une telle situation, les menaces peuvent provenir d'autres clients au sein du service d'informatique en nuage, et les menaces ciblant un client pourraient aussi entraîner des répercussions sur d'autres clients.

b) **Demande provenant d'un dispositif de contrefaçon**: Si une demande provient d'un nuage régional ou en périphérie de contrefaçon, et que le nuage central ne parvient pas à le reconnaître, cela peut entraîner une fuite des données, par exemple.

c) **Attaque d'exécution de script intersites (XSS):** Une attaque d'exécution de script intersites peut être utilisée pour exploiter les vulnérabilités qui existent dans des sites web, en injectant des codes malveillants dans les machines des clients, et les identifiants des utilisateurs sont usurpés pour se livrer à des activités malveillantes.

d) **Enveloppement du langage de balisage extensible (XML)**: Le langage XML est le langage de balisage sous-jacent qui permet l'authentification de l'origine des applications dans le nuage en périphérie. Des hackers peuvent lancer des attaques de piratage de comptes en recourant à des techniques d'enveloppement de signature ou de réécriture XML.

e) **Négligence des employés**: La négligence des employés demeure l'un des plus grands problèmes de sécurité pour tous les systèmes, mais force est de constater que la menace pour la gestion du nuage réparti est particulièrement élevée. Les employés peuvent se connecter à des plates-formes de gestion du nuage réparti depuis leurs téléphones mobiles, leurs appareils domestiques (tablettes et ordinateurs), en exposant potentiellement le système à la merci de nombreuses menaces extérieures.

f) **Hameçonnage et attaques d'ingénierie sociale**: Du fait du caractère ouvert du système en nuage réparti, le hameçonnage et les attaques d'ingénierie sociale se sont généralisés. Une fois que les informations de connexion ou d'autres informations confidentielles sont acquises, un utilisateur malveillant peut potentiellement s'introduire sans difficulté dans le système.

g) **Perte de contrôle**: Lorsque les services d'une organisation sont placés dans le nuage réparti, l'organisation en question perd tout contrôle su ces données et ne sait pas où celles-ci sont stockées dans le nuage. Parallèlement, du point de vue de l'utilisateur, il s'agit d'un grave problème de sécurité dans la mesure où l'utilisateur ne connaît aucun mécanisme de sécurité à même de protéger les services de l'organisation.

h) **Usurpation de l'identité du dispositif**: L'auteur d'une attaque peut se faire passer pour un dispositif légitime et envoyer de fausses données ou des données malveillantes au nuage en périphérie ou voler des données des utilisateurs.

i) **Détournement du dispositif en périphérie**: Il existe de nombreux dispositifs terminaux à proximité du nuage en périphérie qui peuvent collecter des données, transférer des données vers le nuage en périphérie et recevoir des résultats ou des ordres du nuage en périphérie. Un dispositif terminal peut être facilement compromis en raison de son faible niveau de protection de la sécurité.

j) **Attaque par déni de service réparti (DDoS)**: Les attaques DDoS contre les nuages répartis ont considérablement augmenté sur le plan de la viabilité. Si une quantité suffisante de trafic malveillant est émise vers un système d'informatique en nuage, celui-ci peut soit se bloquer complètement, soit rencontrer des difficultés. En particulier, un nuage en périphérie est une entité en nuage relativement plus petite dotée d'une protection de la sécurité relativement

inférieure, raisons pour lesquelles il est plus exposé aux attaques des hackers et utilisé dans le cadre d'attaques DDoS ou d'autres activités illicites.

k) **Sécurité de la virtualisation:** Dans le cadre d'un environnement de nuage en périphérie, la sécurité de la virtualisation comprend la mise en œuvre de l'isolation et du renforcement de la sécurité pour les passerelles, les contrôleurs et les serveurs en périphérie fondés sur les technologies de virtualisation. Par rapport au nuage central et au nuage régional, ces nœuds de périphérie, dont les ressources de stockage et de calcul sont limitées, sont confrontés à des vecteurs d'attaque plus complexes et plus étendus.

8 Lignes directrices relatives à la sécurité du nuage réparti

La présente partie vise à fournir des lignes directrices relatives à la sécurité du nuage central, du nuage régional et du nuage en périphérie, pour des systèmes en nuage répartis, comme indiqué dans le paragraphe 6.

8.1 Lignes directrices relatives à la sécurité du nuage central

Les lignes directrices relatives à la sécurité du nuage central comprennent des lignes directrices concernant la sécurité du système en nuage central, la sécurité physique, la sécurité en cas de déni de service et la sécurité du dispositif en périphérie.

8.1.1 Sécurité du système en nuage central

Les lignes directrices concernant le système en nuage central sont les suivantes:

a) Il est recommandé d'utiliser des outils d'intervention en cas d'incident de vulnérabilité.

b) Il est recommandé d'empêcher les logiciels malveillants de pénétrer dans les services en nuage moyennant des techniques telles que le balayage de fichiers, l'inscription sur liste blanche des applications, la détection de logiciels malveillants fondée sur l'apprentissage automatique et l'analyse du trafic du réseau.

c) Il est recommandé d'examiner et de mettre à jour les évaluations des risques afin d'inclure les services en nuage, et d'identifier et de traiter les facteurs de risque introduits par des environnements et des fournisseurs de nuage central. Des bases de données relatives aux risques pour les fournisseurs de services en nuage sont disponibles en vue d'accélérer le processus d'évaluation.

8.1.2 Sécurité physique

Les lignes directrices concernant la sécurité physique sont les suivantes:

a) Il est recommandé de construire l'infrastructure de nuage centrale à un endroit approprié, plutôt que dans des endroits tels que les pistes d'atterrissage des aéroports, les centrales électriques, les plaines inondables, les lignes de faille des tremblements de terre ou d'autres zones qui sont généralement exposées à des catastrophes naturelles.

b) Il est recommandé de mettre à disposition des processus pour ce qui est du changement, du maintien et de la surveillance des conditions physiques et environnementales pour les infrastructures souterraines.

c) Il est recommandé de mettre à disposition des systèmes de refroidissement et de fournir des normes de conformité pour les infrastructures souterraines.

d) Il est recommandé de limiter les points d'entrée de l'infrastructure en nuage centrale pour réduire les risques d'effractions de nature physique.

e) Il est recommandé de fournir plusieurs points de contrôle dans l'ensemble de l'infrastructure en nuage centrale afin de réduire au minimum les risques d'accès par des intrus malveillants.

f) Il est recommandé, en ce qui concerne un système de contrôle et de surveillance, d'assurer un niveau supplémentaire de sécurité physique.

g) Il est recommandé d'assurer la redondance nécessaire pour aider l'infrastructure en nuage centrale à surmonter tout type d'incident avec un minimum de temps d'arrêt.

8.1.3 Lutte contre le déni de service

Les lignes directrices concernant le déni de service sont les suivantes:

a) Il est recommandé de disposer d'une capacité de serveur dans le nuage central pour gérer les pics de trafic importants et des outils d'atténuation nécessaires pour résoudre les problèmes de sécurité.

b) Il est recommandé d'actualiser et de corriger les pare-feu et le programme de sécurité du réseau régulièrement.

8.2 Lignes directrices relatives au nuage régional

Les lignes directrices concernant le nuage régional comprennent des lignes directrices relatives à la sécurité des données transmises et des données statiques, à la sécurité de l'interface ouverte et à la sécurité de la passerelle IoT.

8.2.1 Sécurité des données transmises et des données statiques

Le nuage régional fournit des services fondés sur le nuage central, partiels ou complets, à une région géographique donnée. Les lignes directrices concernant les données transmises et les données statiques dans le nuage régional sont notamment les suivantes:

a) Il est obligatoire que le nuage régional utilise le chiffrement avec une certaine intensité afin de chiffrer des communications et des données. Il est également recommandé que des services de protocole de transmission sécurisée soient pris en charge pour éviter que des attaques basées sur les protocoles ne nuisent à la confidentialité.

b) Il est obligatoire que le nuage régional authentifie et identifie les identités des services, et que des stratégies strictes d'isolation de la sécurité et de contrôle d'accès soient adoptées. Il est obligatoire de prendre en charge la personnalisation et la gestion des stratégies de contrôle d'accès.

c) Il est recommandé que le nuage régional prenne en charge un système d'échange des données sécurisé, afin de surveiller et de contrôler en temps réel le format, le contenu et le flux de données, etc.

d) Il est recommandé que le système d'échange des données sécurisé répond à diverses exigences d'élasticité dans l'environnement en nuage, notamment en ce qui concerne la fourniture de méthodes de déploiement souples, de modes de programmation des ressources souples et de méthodes sécurisées d'échange des données reposant sur l'isolation de la sécurité fondée sur les opérations, etc.

e) Il est recommandé que le nuage régional prenne en charge la détection des codes malveillants et la suppression des données transmises.

f) Il est obligatoire d'adopter des mécanismes de chiffrement et de vérification pour garantir l'intégrité et la confidentialité du stockage local, y compris les données de gestion du système (fichiers d'index, informations et clés concernant le service en nuage, par exemple), les informations d'authentification et les données opérationnelles importantes (telles que les données relatives à la vie privée des utilisateurs).

g) Il est recommandé de prendre en charge l'authentification de l'identité basée sur le rôle pour accéder aux données, et d'appliquer des mesures de contrôle d'accès strictes afin de lutter contre les accès illégaux.

8.2.2 Sécurité de l'interface ouverte

Le fournisseur CSP doit fournir des interfaces de réseau et des interfaces de programmation d'application (API) afin de pouvoir configurer, gérer, coordonner et surveiller différents services en nuage, et également de fournir des services sans intermédiaire. Généralement, les tierces parties évoluent pour fournir des services additionnels sur la base de ces interfaces. Les lignes directrices concernant les interfaces API sécurisées du nuage régional sont les suivantes:

a) Il est obligatoire d'utiliser le chiffrement, tel que la sécurité de la couche transport (TLS) ou d'autres méthodes de chiffrement, pour qu'une interface API fondée sur le transfert d'état représentationnel (REST) puisse chiffrer des données durant la transmission et éviter l'altération volontaire des données. Il est également obligatoire d'utiliser un mécanisme de signature pour s'assurer que seuls les utilisateurs ayant des droits d'accès peuvent déchiffrer et modifier les données.

b) Il est recommandé de définir des identités fiables pour les interfaces API au moyen de jetons, puis de faire en sorte que seules les identités fiables avec jeton puissent accéder aux services et aux ressources de données, entre autres, et les contrôler.

c) Il est recommandé d'effectuer une surveillance en temps réel et d'émettre des avertissements concernant les comportements d'appel de l'interface API ouverte et la transmission anormale de données, par exemple en limitant la fréquence d'accès à l'interface API.

d) Il est recommandé d'identifier activement les vulnérabilités des interfaces API. On pourrait utiliser des outils de détection pour repérer des failles dans la sécurité des interfaces API et des fuites de données, et pour savoir si les interfaces API ont été attaquées et si des vulnérabilités sont exploitées en temps réel.

e) Il est recommandé d'utiliser des passerelles de sécurité des interfaces API étant donné que la passerelle de sécurité des interfaces API constitue une technologie essentielle pour protéger la sécurité des interfaces API. Puisque la passerelle de sécurité des interfaces API peut être utilisée pour contrôler et gérer l'utilisation de ces interfaces, elle peut également authentifier les utilisateurs qui utilisent les interfaces API et les services associés.

8.2.3 Sécurité de la passerelle IoT

Les dispositifs IoT se connectent à l'Internet via les passerelles IoT, lesquelles deviennent les cibles privilégiées des logiciels malveillants et des attaques de réseau. Les lignes directrices concernant la sécurité des passerelles IoT sont les suivantes:

a) Il est recommandé que les passerelles IoT prennent en charge l'authentification du dispositif et le contrôle d'accès; seuls les utilisateurs et les dispositifs autorisés se voient accorder un accès et mettent en œuvre un stockage ou des coffres-forts sécurisés afin de protéger des informations confidentielles, comme des clés ou des certificats.

b) Il est recommandé que les passerelles IoT prennent en charge la gestion des politiques pour configurer les droits d'accès et contrôler l'accès du dispositif aux services d'application (services techniques, services opérationnelles et services de données), aux fichiers (fichiers de configuration, fichiers journaux et fichiers miroirs) et à d'autres objets conformément aux politiques de sécurité, et que les passerelles soient en mesure d'interrompre des connexions et des sessions illégales à temps.

c) Il est recommandé que les passerelles IoT permettent une mise à jour hertzienne (OAT) afin de s'assurer que la passerelle exécute les derniers logiciels et micrologiciels, ce qui permet d'éviter des vulnérabilités et des risques courants. Le démarrage sécurisé peut permettre de s'assurer que la passerelle est amorcée avec une image de micrologiciel dont l'intégrité et l'authenticité ont été chiffrées et vérifiées, empêchant ainsi l'utilisation de micrologiciels malveillants pour démarrer la passerelle.

d) Il est recommandé que les passerelles IoT prennent en charge diverses mesures de contrôle de la sécurité pour protéger les dispositifs IoT. Par exemple, lorsqu'une passerelle IoT est utilisée en tant que serveur tampon de sécurité pour les réseaux et les dispositifs, il est recommandé que les pare-feu ainsi que les fonctions de filtrage du trafic basé sur la règle et de mise sur liste blanche soient exécutés dans la passerelle.

e) Il est recommandé que les passerelles IoT prennent en charge des journaux d'événements affinés, afin d'avoir une compréhension approfondie des processus exécutés dans la passerelle aux fins des audits de sécurité.

8.3 Lignes directrices relatives à la sécurité du nuage en périphérie

Les lignes directrices concernant le nuage en périphérie comprennent des lignes directrices relatives à la sécurité de l'infrastructure de nuage en périphérie, la sécurité du réseau de nuage en périphérie pour les données transmises et les données statiques, la sécurité du web et la sécurité des dispositifs terminaux à proximité du nuage en périphérie.

8.3.1 Sécurité de l'infrastructure de nuage en périphérie

L'infrastructure de nuage en périphérie fournit des bases aussi bien matérielles que logicielles, et la sécurité de l'infrastructure en périphérie est un élément essentiel du nuage en périphérie. Les lignes directrices relatives à la sécurité de l'infrastructure de nuage en périphérie sont les suivantes:

a) Il est recommandé de mettre à disposition un cadre de virtualisation léger et indépendant du matériel et de mettre en œuvre l'isolation de la sécurité et le renforcement des mécanismes.

b) Il est recommandé de renforcer la protection de la sécurité de l'hyperviseur et de réduire les vecteurs d'attaque.

c) Il est recommandé de coopérer avec les serveurs en nuage en périphérie et de procéder à la détection des codes malveillants du service d'exploitation et à la prévention à cet égard, ainsi qu'à l'isolation renforcée de la sécurité des applications, de prendre en charge des environnements d'exécution fiables et d'autres mécanismes importants, afin de garantir la confidentialité et l'intégrité des applications fonctionnant sur le système d'exploitation, qui pâtissent de ressources informatiques ou de ressources de stockage limitées, et du fait que la synchronisation des mécanismes et des politiques de sécurité puisse ne pas avoir lieu à temps avec le nuage central ou régional.

d) Il est recommandé que les fournisseurs de services fondés sur le nuage en périphérie mettent en œuvre des processus d'identification et d'authentification de manière automatique, transparente et simple. En effet, les nœuds de périphérie et la structure de réseau dynamique du nuage réparti peuvent entraîner la répétition de l'identification et de l'authentification.

8.3.2 Sécurité du réseau fondé sur le nuage en périphérie

Compte tenu des nombreux nœuds de périphérie et de la topologie de réseau complexe, qui est de nature à accroître les parcours d'attaque, les auteurs des attaques peuvent facilement envoyer des paquets de réseau malveillants aux nœuds de nuage en périphérie ou lancer des attaques par déni de service, qui mettent à mal la fiabilité du réseau fondé sur le nuage en périphérie. Les lignes directrices concernant le réseau fondé sur le nuage en périphérie sont les suivantes:

a) Il est recommandé de garantir la sécurité du protocole, tant au stade de la conception qu'au stade de la mise en œuvre, à laquelle le nuage en périphérie a recours pour répondre à diverses exigences en matière de transmission de données pour les consommateurs CSC.

b) Il est recommandé d'ajouter des politiques de sécurité pour les protocoles potentiellement vulnérables, par exemple en transmettant les données par le biais d'un réseau virtuel privé (VPN), d'une couche TLS ou d'autres voies sécurisées moyennant l'ajout de modules dans les passerelles.

c) Il est recommandé d'effectuer des vérifications de l'intégrité et de la sécurité pour la transmission du réseau entre des machines virtuelles qui appartiennent à différents domaines, afin de garantir une isolation efficace entre les différentes unités de communication de l'entité. En outre, les modules d'isolation peuvent être programmés par des contrôleurs dans l'environnement visualisé en vue de fournir des capacités d'isolation.

d) Il est recommandé de surveiller la sécurité sur le trafic de réseau afin de prévenir les événements de sécurité à temps et d'intervenir rapidement en cas d'incident. De plus, les systèmes de protection peuvent bloquer directement le trafic malveillant.

8.3.3 Sécurité du web fondé sur le nuage en périphérie

Les lignes directrices concernant la sécurité du web sont les suivantes:

a) Il est recommandé d'assurer une surveillance à distance efficace des installations d'un système fondé sur le nuage en périphérie.

b) Il est recommandé que la sécurité du nuage en périphérie aille de pair avec des initiatives considérables de sensibilisation. Les employés sont informés de ce qu'ils peuvent et ne peuvent pas faire avec leurs appareils et sont aidés à identifier les risques de sécurité.

c) Il est recommandé de veiller à ce que les appareils anciens et obsolètes ne soient pas placés à côté d'appareils plus sophistiqués afin de réduire les points de vulnérabilité au sein du réseau.

8.3.4 Sécurité des dispositifs terminaux dans le nuage en périphérie

Les lignes directrices concernant la sécurité des dispositifs terminaux dans le nuage en périphérie sont les suivantes:

a) Il est recommandé de bloquer l'accès lorsqu'un appareil personnel non autorisé tente d'accéder aux données du nuage en périphérie.

b) Il est recommandé de configurer l'environnement de nuage en périphérie avec des fonctionnalités telles que l'authentification forte et les nœuds d'authentification cryptés.

c) Il est recommandé que les protocoles de sécurité informatique gèrent les dispositifs qui peuvent accéder au réseau du système fondé sur le nuage en périphérie et les conditions de cet accès.

d) Il est recommandé de mettre en œuvre et de surveiller en permanence l'environnement de nuage en périphérie.

e) Il est recommandé de partir du principe que les dispositifs de périphérie sont déjà compromis plutôt que de faire automatiquement confiance aux informations provenant d'un dispositif, toutes les données pouvant être malveillantes jusqu'à preuve du contraire.

f) Il est recommandé que seuls les dispositifs de périphérie authentifiés puissent se connecter et transmettre des données au nuage central.

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	Équipements 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, 2023