Union internationale des télécommunications

UIT-T

SECTEUR DE LA NORMALISATION
DES TÉLÉCOMMUNICATIONS
DE L'UIT

X.1604

(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 relatives au réseau en tant que service (NaaS) dans l'informatique en nuage

Recommandation UIT-T X.1604

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.1604

## Exigences de sécurité relatives au réseau en tant que service (NaaS) dans l'informatique en nuage


### Résumé

La Recommandation UIT-T X.1604 vise à analyser les menaces et les problèmes de sécurité concernant le réseau en tant que service (NaaS) dans l'informatique en nuage, et précise les exigences de sécurité relatives aux aspects du NaaS, à savoir les applications NaaS, les plates-formes NaaS et la connectivité NaaS, sur la base des types de capacités de nuage correspondants.



### Historique

| Édition | Recommandation | Approbation | Commission d'études | ID unique* |
|---|---|---|---|---|
| 1.0 | UIT-T X.1604 | 26-03-2020 | 17 | 11.1002/1000/14093 |

### Mots clés

Nuage, réseau en tant que service, exigences de 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 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

# Recommandation UIT-T X.1604

## Exigences de sécurité relatives au réseau en tant que service (NaaS) dans l'informatique en nuage

### 1 Champ d'application

La présente Recommandation vise à analyser les menaces et les problèmes de sécurité concernant le réseau en tant que service (NaaS) dans l'informatique en nuage, et précise les exigences de sécurité relatives aux aspects du NaaS, à savoir les applications NaaS, les plates-formes NaaS et la connectivité NaaS, sur la base des types de capacités de nuage correspondants.

### 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. Les Recommandations et autres références étant sujettes à révision, les utilisateurs de la présente Recommandation sont invités à rechercher la possibilité d'appliquer les éditions les plus récentes des Recommandations et autres références énumérées ci-dessous. Une liste des Recommandations UIT-T en vigueur est publiée périodiquement. La référence à un document figurant dans la présente Recommandation ne donne pas à ce document, en tant que tel, le statut de Recommandation.

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

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

[UIT-T Y.3512] Recommandation UIT-T Y.3512 (2014), *Informatique en nuage – Exigences fonctionnelles relatives au réseau en tant que service*.

### 3 Définitions

#### 3.1 Termes définis ailleurs

La présente Recommandation utilise les termes suivants définis ailleurs:

**3.1.1 contrôle d'accès** [b-UIT-T X.800]: précaution prise contre l'utilisation non autorisée d'une ressource; cela comprend les précautions prises contre l'utilisation d'une ressource de façon non autorisée.

**3.1.2 authentification** [b-ISO/CEI 18014-2]: garantie donnée concernant l'identité d'une entité.

**3.1.3 autorisation** [b-UIT-T X.1251]: le service d'autorisation est chargé de la prise de décisions concernant les droits d'accès de l'utilisateur et l'application des décisions en matière d'autorisation, en fonction des privilèges de l'utilisateur. L'autorisation est un service facultatif, qui n'est fourni que lorsque l'accès aux ressources doit être contrôlé en fonction des droits de l'utilisateur.

**3.1.4 confidentialité** [b-UIT-T X.800]: propriété d'une information qui n'est ni disponible, ni divulguée aux personnes, entités ou processus non autorisés.

**3.1.5 intégrité des données** [b-UIT-T X.800]: propriété assurant que des données n'ont pas été modifiées ou détruites de façon non autorisée.

**3.1.6 pare-feu** [b-ISO/CEI 27033-1]: type de barrière de sécurité placée entre des environnements de réseau, qui se présente sous la forme d'un dispositif dédié ou d'un ensemble de plusieurs composants et techniques, à travers laquelle passe tout le trafic d'un environnement de réseau à un autre et vice versa. Seul le trafic autorisé défini dans le cadre d'une politique de sécurité locale est autorisé à passer.

**3.1.7 système de détection des intrusions** [b-ISO/CEI 27039]: systèmes d'information utilisés pour déterminer qu'une tentative d'intrusion a eu lieu ou qu'une intrusion est en cours ou a eu lieu.

**3.1.8 clé** [b-UIT-T X.800]: série de symboles commandant les opérations de chiffrement et de déchiffrement.

**3.1.9 gestion de clés** [b-UIT-T X.800]: production, stockage, distribution, suppression, archivage et application de clés conformément à la politique de sécurité.

**3.1.10 certificat de clé publique (PKC)** [b-UIT-T X.509]: clé publique d'une entité, associée à d'autres informations, qui est rendue infalsifiable par signature numérique en utilisant la clé privée de l'autorité de certification émettrice.

**3.1.11 menace** [b-ISO/CEI 27000]: cause potentielle d'un incident indésirable, qui peut nuire à un système ou à un organisme.

### 3.2 Termes définis dans la présente Recommandation

Aucun.

## 4 Abréviations et acronymes

La présente Recommandation utilise les abréviations et acronymes suivants:

BoD bande passante à la demande *(bandwidth on demand)*

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)*

DoS déni de service *(denial of service)*

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

SNMP protocole simple de gestion de réseau (*simple network management protocol*)

vCDN réseau virtuel de fourniture de contenu *(virtual content delivery network)*

vEPC réseau central évolué en mode paquet virtualisé *(virtualized evolved packet core)*

vFW pare-feu virtuel *(virtual firewall)*

VPN réseau privé virtuel *(virtual private network)*

## 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.

L'expression "**il est interdit**" 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 "**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 service 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.

## 6 Aperçu

Selon la Recommandation [UIT-T Y.3500], une catégorie de services en nuage est un groupe de services en nuage possédant un ensemble commun de caractéristiques. Le réseau en tant que service (NaaS) est l'une des catégories de services en nuage pour laquelle la capacité fournie au client de services en nuage (CSC) correspond à des capacités de connectivité de transport et à des capacités de réseau connexes.

Comme indiqué dans la Recommandation [UIT-T Y.3512], les services NaaS peuvent fournir l'un quelconque des trois types de capacités de nuage suivants: service d'application NaaS, service de plate-forme NaaS et service de connectivité NaaS.

- **Le service d'application NaaS** offre aux clients CSC des applications de réseau en nuage, par exemple un routeur virtuel, un réseau virtuel de fourniture de contenu (vCDN), un réseau central évolué en mode paquet virtualisé (vEPC) ou un pare-feu virtuel (vFW).
- **Le service de plate-forme NaaS** fournit aux clients CSC une plate-forme de réseau qui offre un environnement programmable pour les fonctionnalités de réseau.
- **Le service de connectivité NaaS** offre aux clients CSC la possibilité de fournir et d'utiliser des ressources de connectivité de réseau, par exemple un réseau privé virtuel (VPN) flexible et étendu, une bande passante à la demande (BoD), etc.

Le concept de haut niveau du réseau NaaS peut être schématisé comme indiqué dans la Figure 1:

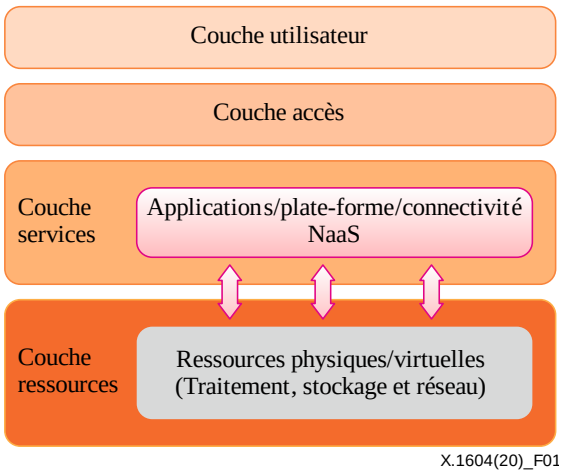


**Figure 1 – Concept de haut niveau du réseau NaaS**

En utilisant ces trois types de services de réseau, le NaaS peut offrir des fonctions de réseau dans l'informatique en nuage, dont la coordination de la virtualisation des capacités de calcul et de stockage avec les capacités de réseau, la commande harmonisée de technologies de réseau hétérogènes et la reconfiguration à la demande.

Cependant, le NaaS est confronté à plusieurs problèmes de sécurité:

- **Menaces et problèmes de sécurité relatifs aux applications NaaS**: un service d'application NaaS vise à fournir aux clients CSC, par l'intermédiaire d'un fournisseur CSP, des

applications de réseau virtuel, par exemple un pare-feu virtuel (vFW), un routeur virtuel, un réseau virtuel de fourniture de contenu (vCDN), etc. Le service d'application NaaS est confronté à des problèmes de sécurité relatifs aux vulnérabilités des applications sur le plan de la sécurité, aux risques liés à la sécurité de la virtualisation de réseau, à l'utilisation en partage des équipements de réseau physiques, etc.

- **Menaces et problèmes de sécurité relatifs aux plates-formes NaaS**: un service de plate-forme NaaS vise à offrir aux clients CSC, par l'intermédiaire d'un fournisseur CSP, des environnements logiciels et une plate-forme pour gérer, déployer et exécuter des applications de réseau. Les problèmes de sécurité concernant les plates-formes NaaS incluent, sans toutefois s'y limiter, les attaques par DoS visant les plates-formes de réseau, les vulnérabilités des systèmes d'exploitation sur le plan de la sécurité, les violations de contrôle d'accès, etc.
- **Menaces et problèmes de sécurité relatifs à la connectivité NaaS**: un service de connectivité NaaS vise à fournir aux clients CSC, par l'intermédiaire d'un fournisseur CSP, une connexion au réseau, par exemple un réseau privé virtuel (VPN), une bande passante à la demande (BoD), etc. L'apparition d'un problème de sécurité au niveau du service de connectivité crée des risques non seulement pour les services NaaS, mais aussi pour d'autres ressources en nuage et pour les données des clients CSC. Les problèmes de sécurité relatifs au service de connectivité NaaS incluent, sans toutefois s'y limiter, les écoutes illicites, les attaques de l'intercepteur, etc.

La présente Recommandation vise à analyser les exigences de sécurité concernant le NaaS dans l'informatique en nuage, en particulier les applications NaaS, les plates-formes NaaS et la connectivité NaaS.

## 7 Menaces et problèmes de sécurité relatifs au réseau en tant que service dans l'informatique en nuage

Les paragraphes 7 et 8 de la Recommandation [UIT-T X.1601] traitent respectivement des menaces et des problèmes de sécurité concernant les clients CSC et les fournisseurs CSP dans l'informatique en nuage. Le NaaS dans l'informatique en nuage est aussi confronté à des menaces et à des problèmes de sécurité semblables à ceux définis dans la Recommandation [UIT-T X.1601], qui sont indiqués ci-dessous:

a) vulnérabilités des systèmes;

b) perte et fuite de données;

c) accès non sécurisé aux services;

d) accès non autorisé aux fonctions d'administration;

e) menaces internes;

f) perte de confiance;

g) perte de gouvernance;

h) perte de confidentialité;

i) indisponibilité des services; et

j) environnement partagé.

Le NaaS dans l'informatique en nuage est confronté à des menaces et à des problèmes propres à chaque capacité de nuage.

### 7.1 Menaces et problèmes de sécurité relatifs aux applications NaaS

a) Vulnérabilités du réseau et des systèmes: de possibles vulnérabilités en matière de sécurité des applications NaaS pourraient être exploitées par des auteurs d'attaques. Les défauts techniques de la virtualisation des applications NaaS pourraient présenter plusieurs risques

sur le plan de la sécurité; en outre, ces risques pourraient être aggravés si les techniques d'exploitation et de maintenance ne sont pas suffisamment au point.

b) Utilisation en partage des équipements de réseau physiques: le partage des équipements de réseau physiques pourrait entraîner la perte, la fuite ou l'utilisation abusive de données sur un équipement utilisé en partage.

c) Accès non sécurisé: l'accès non sécurisé aux applications NaaS pourrait entraîner la perte, la fuite ou l'utilisation abusive de données des applications.

d) Accès non autorisé aux fonctions d'administration: l'accès non autorisé aux fonctions d'administration d'une application NaaS pourrait conduire à une perte de données.

e) Indisponibilité d'une application: une application NaaS peut faire l'objet d'une attaque par déni de service (DoS) ou par déni de service réparti (DDoS); en outre, une attaque pourrait endommager l'équipement matériel et entraîner la perte ou la destruction de données.

### 7.2 Menaces et problèmes de sécurité relatifs aux plates-formes NaaS

a) Attaques par DoS visant une plate-forme de réseau: lorsqu'une ou plusieurs plates-formes ont fait l'objet d'une attaque par DoS, ces plates-formes et d'autres plates-formes virtualisées ne peuvent répondre à cause de la consommation des ressources du processeur et de la mémoire en transition.

b) Vulnérabilités en matière de sécurité du système d'exploitation: les données sur les plates-formes NaaS pourraient être perdues; en outre, les vulnérabilités en matière de sécurité des systèmes d'exploitation pourraient conduire à une propagation de virus et à d'autres risques graves sur le plan de la sécurité.

c) Violation de contrôle d'accès: la violation de contrôle d'accès peut entraîner la perte, la fuite ou l'utilisation abusive de données.

d) Indisponibilité de la plate-forme de réseau: l'indisponibilité d'une plate-forme NaaS pourrait rendre les services NaaS indisponibles; il se peut donc que les applications Naas connexes et le service de connectivité NaaS ne fonctionnent pas non plus.

e) Accès non autorisé aux fonctions d'administration: l'accès non autorisé aux fonctions d'administration d'une plate-forme NaaS pourrait entraîner la perte, la fuite ou l'utilisation abusive de données. L'auteur d'une attaque peut, par exemple, exploiter une vulnérabilité du système pour obtenir un accès non autorisé aux fonctions d'administration de la plate-forme NaaS et remplacer l'adresse IP de destination de la collecte des données par sa propre adresse IP.

f) Menaces internes venant d'un employé: si un client bénéficiant de services NaaS est une entreprise ou une organisation, et non une personne, les employés de cette organisation partagent des mots de passe "administrateur", ce qui est également le cas du fournisseur de services NaaS. Les utilisateurs négligents ou mal formés (ou les membres d'une famille dans le cas d'une configuration chez des particuliers) ou encore des actions malveillantes de la part d'employés mécontents, représenteront toujours une menace importante.

### 7.3 Menaces et problèmes de sécurité relatifs à la connectivité NaaS

a) Écoutes illicites: les données de connexion et de transmission pourraient faire l'objet d'écoutes illicites de la part des auteurs d'attaques.

b) Attaques lors de la connexion au réseau: des attaques de réseau peuvent se produire lors de la connexion au réseau, comme des attaques d'intercepteur, des attaques par DoS, etc.

c) Perte et fuite de données: en utilisant les services NaaS, les clients NaaS utilisent habituellement le réseau fourni par les fournisseurs NaaS pour le transport de données. Ces données peuvent être des données personnelles et des secrets commerciaux ou porter sur des questions politiques. La fuite de données constitue donc une menace sérieuse pour les utilisateurs NaaS.

d) Usurpation d'identité: des auteurs d'attaques peuvent se faire passer pour le système de gestion ou le serveur de stockage des données du NaaS de l'informatique en nuage et provoquer la perte de données de connexion ou de transmission.

e) Interception et falsification: un équipement de réseau endommagé, l'intrusion d'un pirate et la faillite d'un fournisseur de services NaaS risquent d'entraîner une perte de données qui ne peuvent plus être récupérées. En outre, des pirates peuvent aussi falsifier des données s'ils parviennent à entrer dans le réseau.

f) Accès non sécurisé au réseau: un accès non sécurisé au réseau pourrait entraîner la perte, la fuite ou l'utilisation abusive de données de connexion ou de transmission.

g) Authentification d'identité non sécurisée: une authentification d'identité non sécurisée pourrait entraîner la perte, la fuite ou l'utilisation abusive de données de connexion ou de transmission.

h) Indisponibilité du réseau: le réseau de connectivité NaaS pourrait faire l'objet d'une attaque par DoS ou DDoS; en outre, les attaques par DoS ou DDoS pourraient entraîner une panne des serveurs du NaaS dans l'informatique en nuage.

i) Vulnérabilité de l'interface d'acquisition: des auteurs d'attaques peuvent exploiter les vulnérabilités de l'interface d'acquisition de données de surveillance.

j) Accès non autorisé aux fonctions d'administration: l'accès non autorisé aux fonctions d'administration d'un système de connectivité NaaS pourrait provoquer une perte de données de transmission.

# 8 Exigences de sécurité relatives au réseau en tant que service dans l'informatique en nuage

Ce paragraphe vise à identifier les exigences de sécurité relatives au NaaS dans l'informatique en nuage.

## 8.1 Exigences de sécurité relatives aux applications NaaS

Les exigences de sécurité relatives aux applications NaaS sont les suivantes:

a) Il est obligatoire de préserver l'intégrité et l'exactitude des données des applications NaaS.

b) Il est recommandé de disposer de méthodes de contrôle d'accès aux données des applications NaaS, par exemple d'une liste blanche, d'une liste noire, etc.

c) Il est recommandé que le fournisseur CSP mette à la disposition des clients CSC des méthodes de contrôle d'accès appropriées, par exemple une liste blanche, une liste noire, un compte et un mot de passe, etc. pour empêcher les utilisateurs non autorisés d'avoir accès aux systèmes ou aux données. Les solutions courantes de contrôle d'accès applicables à l'informatique en nuage figurent dans la Recommandation [UIT-T X.1601].

d) Il est obligatoire que le fournisseur CSP prévoie la journalisation et l'audit de l'utilisation des applications NaaS.

e) Il est obligatoire que le fournisseur CSP mette en place des mesures de protection contre les vulnérabilités du système des applications NaaS; le fournisseur CSP pourrait, par exemple, utiliser des méthodes de test d'intrusion pour prévenir les vulnérabilités du système des applications NaaS.

f) Il est obligatoire que le fournisseur CSP dispose de méthodes de sauvegarde pour prévenir la perte de données des applications NaaS, comme la sauvegarde au moyen de disques physiques, les méthodes de stockage réparti des données, etc. Les méthodes courantes de sauvegarde sont définies dans la Recommandation [UIT-T X.1601].

Le Tableau 8-1 fournit un résumé mettant en correspondance les menaces de sécurité liées aux applications NaaS et les exigences de sécurité.

**Tableau 8-1 – Applications NaaS: mise en correspondance des menaces de sécurité et des exigences de sécurité**

| Menaces de sécurité | Exigences de sécurité |
|---|---|
| Vulnérabilités en matière de sécurité des applications | b), d), e), f) |
| Risques relatifs à la sécurité de la virtualisation du réseau | a), b), c), d), f) |
| Utilisation en partage des équipements de réseau physiques | a), b), c), d), f) |
| Accès non sécurisé | b), c), d), e), f) |
| Accès non autorisé aux fonctions d'administration | b), c), d), f) |
| Indisponibilité des applications | d), e), f) |

## 8.2 Exigences de sécurité relatives aux plates-formes NaaS

Les exigences de sécurité relatives aux plates-formes NaaS sont les suivantes:

a) Il est obligatoire de préserver l'intégrité et l'exactitude des données des plates-formes NaaS.

b) Il est recommandé de disposer de méthodes de contrôle d'accès aux données des plates-formes NaaS, par exemple d'une liste blanche, d'une liste noire, etc.

c) Il est recommandé que le fournisseur CSP mette à la disposition des clients CSC des méthodes de contrôle d'accès appropriées, par exemple une liste blanche, une liste noire, un compte et un mot de passe, etc. pour empêcher les utilisateurs non autorisés d'avoir accès aux systèmes ou aux données. Les solutions courantes de contrôle d'accès applicables à l'informatique en nuage sont définies dans la Recommandation [UIT-T X.1601].

d) Il est obligatoire que le fournisseur CSP prévoie la journalisation et l'audit de l'utilisation des plates-formes NaaS.

e) Il est obligatoire que le fournisseur CSP mette en place des mesures de protection contre les vulnérabilités du système des plates-formes NaaS; le fournisseur CSP devrait, par exemple, prévenir la perte et la fuite de données des plates-formes NaaS.

f) Il est obligatoire que le fournisseur CSP dispose de méthodes de sauvegarde pour prévenir la perte de données des plates-formes NaaS, comme la sauvegarde au moyen de disques physiques, les méthodes de stockage réparti des données, etc. Les méthodes courantes de sauvegarde sont définies dans la Recommandation [UIT-T X.1601].

Le Tableau 8-2 fournit un résumé mettant en correspondance les menaces de sécurité liées aux plates-formes NaaS et les exigences de sécurité.

**Tableau 8-2 – Plates-formes NaaS: mise en correspondance des menaces de sécurité et des exigences de sécurité**

| Menaces de sécurité | Exigences de sécurité |
|---|---|
| Attaque par DoS visant une plate-forme du réseau | a), b), c), d), e), f) |
| Vulnérabilités en matière de sécurité du système d'exploitation | a), b), d), e), f) |
| Violation de contrôle d'accès | a), b), c), d), e), f) |
| Indisponibilité de la plate-forme du réseau | a), d), e), f) |
| Accès non autorisé aux fonctions d'administration | b), c), d), f) |
| Menaces internes venant des employés | b), d), f) |

### 8.3 Exigences de sécurité relatives à la connectivité NaaS

Les exigences de sécurité relatives à la connectivité NaaS sont les suivantes:

a) Il est obligatoire de préserver l'intégrité et l'exactitude des données de connectivité NaaS.

b) Il est recommandé de disposer de méthodes de contrôle d'accès aux interfaces de la connectivité NaaS, par exemple d'une liste blanche, d'une liste noire, etc.

c) Il est recommandé de disposer de méthodes cryptographiques pour assurer la sécurité des données de connexion et de transmission.

d) Il est recommandé d'utiliser des protocoles réseau classiques entre les ressources en nuage et les serveurs du service de connectivité NaaS, comme le protocole simple de gestion de réseau (SNMP) ou d'autres protocoles réseau classiques.

e) Il est recommandé que le fournisseur CSP mette à la disposition des clients CSC des méthodes de contrôle d'accès appropriées, par exemple une liste blanche, une liste noire, un compte et un mot de passe, etc. pour empêcher les utilisateurs non autorisés d'avoir accès aux systèmes ou aux données. Les solutions courantes de contrôle d'accès applicables à l'informatique en nuage sont définies dans la Recommandation [UIT-T X.1601].

f) Il est obligatoire que le fournisseur CSP prévoie la journalisation et l'audit de l'utilisation de la connectivité NaaS.

g) Il est obligatoire que le fournisseur CSP mette en œuvre des méthodes d'authentification pour protéger l'accès aux données du service de connectivité NaaS, comme une authentification à deux facteurs ou d'autres méthodes. Les méthodes courantes d'authentification applicables à l'informatique en nuage sont définies dans la Recommandation [UIT-T X.1601].

h) Il est obligatoire que le fournisseur CSP mette en place des mesures de protection contre les vulnérabilités du système de connectivité NaaS. Le fournisseur CSP pourrait, par exemple, utiliser des méthodes de test d'intrusion pour prévenir les vulnérabilités du système de connectivité NaaS.

Le Tableau 8-3 fournit un résumé mettant en correspondance les menaces de sécurité liées à la connectivité NaaS et les exigences de sécurité.

**Tableau 8-3 – Connectivité NaaS: mise en correspondance des menaces de sécurité et des exigences de sécurité**

| Menaces de sécurité | Exigences de sécurité |
|---|---|
| Écoutes illicites | b), c), d), e), f), g) h) |
| Attaque lors de la connexion au réseau | d), f), h) |
| Perte et fuite de données | a), b), c), d), e), f), g) h) |
| Usurpation d'identité | a), b), d), e), f), g) h) |
| Interception et falsification | a), b), c), d), e), f), g) h) |
| Accès non sécurisé au réseau | b), c), d), e), f), g) h) |
| Authentification d'identité non sécurisée | b), c), e), f), g) h) |
| Indisponibilité du réseau | d), f), h) |
| Vulnérabilité de l'interface d'acquisition | a), b), c), d), f), h) |
| Accès non autorisé aux fonctions d'administration | c), f), g) |

# Bibliographie


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

[b-UIT-T X.509] Recommandation UIT-T X.509 (2019) | ISO/CEI 9594-8:2020, *Technologies de l'information – Interconnexion des systèmes ouverts – L'annuaire: cadre général des certificats de clé publique et d'attribut*.

[b-UIT-T X.800] Recommandation UIT-T X.800 (1991) | ISO/CEI 7498-2:1989, *Architecture de sécurité pour l'interconnexion en systèmes ouverts d'applications du CCITT*.

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

[b-UIT-T X.1251] Recommandation UIT-T X.1251 (2019), *Cas d'utilisation pour l'expression structurée d'informations sur les menaces*.

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

[b-ISO/CEI 18014-2] ISO/CEI 18014-2:2009, *Technologies de l'information – Techniques de sécurité – Services d'horodatage – Partie 2: Mécanismes produisant des jetons indépendants*.

[b-ISO/CEI 19440] ISO/CEI 19440:2007, *Entreprise intégrée – Constructions pour la modélisation d'entreprise*.

[b-ISO/CEI 19944] ISO/CEI 19944:2017, *Technologies de l'information – Informatique en nuage – Services et dispositifs en nuage: débits, catégories et utilisation des données*.

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

[b-ISO/CEI 27000] ISO/CEI 27000:2018, *Technologies de l'information – Techniques de sécurité – Systèmes de management de la sécurité de l'information – Vue d'ensemble et vocabulaire*.

[b-ISO/CEI 27033-1] ISO/CEI 27033-1:2015, *Technologies de l'information – Techniques de sécurité – Sécurité de réseau – Partie 1: Vue d'ensemble et concepts*.

[b-ISO/CEI 27039] ISO/CEI 27039:2015, *Technologies de l'information – Techniques de sécurité – Sélection, déploiement et opérations des systèmes de détection et prévention d'intrusion*.

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

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

## 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