Union internationale des télécommunications

UIT-T

SECTEUR DE LA NORMALISATION
DES TÉLÉCOMMUNICATIONS
DE L'UIT

X.1369

(01/2022)

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

Applications et services sécurisés (2) – Sécurité de l'Internet des objets (IoT)

Exigences de sécurité pour la plate-forme de services IoT

Recommandation UIT-T X.1369

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	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.1369

Exigences de sécurité pour la plate-forme de services IoT

Résumé

La Recommandation UIT-T X.1369 indique les exigences de sécurité applicables à la plate-forme de services de l'Internet des objets (IoT). Elle permet d'évaluer les menaces et les problèmes de sécurité pour la plate-forme de services commerciaux IoT et décrit les mesures de sécurité permettant d'atténuer ces menaces et ces problèmes.

Historique

Édition	Recommandation	Approbation	Commission d'études	Identifiant unique*
1.0	UIT-T X.1369	07-01-2022	17	11.1002/1000/14799

Mots clés

Internet des objets (IoT), plate-forme de services, exigences de sécurité, risques 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 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.1369

Exigences de sécurité pour la plate-forme de services IoT

1 Domaine d'application

La présente Recommandation indique les exigences de sécurité applicables à la plate-forme de services de l'Internet des objets (IoT). Elle permet d'évaluer les menaces et les problèmes de sécurité pour la plate-forme de services IoT et décrit les mesures de sécurité permettant d'atténuer ces menaces et ces problèmes.

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 tout texte étant sujet à révision, les utilisateurs de la présente Recommandation sont invités à se reporter, si possible, aux versions les plus récentes des références normatives suivantes. 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.

[ISO/CEI 30141] ISO/CEI 30141 (2018), *Architecture de référence de l'Internet des objets*.

3 Définitions

3.1 Termes définis ailleurs

La présente Recommandation utilise le terme suivant défini ailleurs:

3.1.1 Internet des objets (IoT) [b-UIT-T Y.4000]: infrastructure mondiale pour la société de l'information, qui permet de disposer de services évolués en interconnectant des objets (physiques ou virtuels) grâce aux technologies de l'information et de la communication interopérables existantes ou en évolution.

3.2 Termes définis dans la présente Recommandation

La présente Recommandation définit le terme suivant:

3.2.1 plate-forme de services IoT: plate-forme à laquelle des dispositifs IoT sont connectés et sur laquelle des applications IoT sont exécutées.

Sur le plan fonctionnel, la plate-forme de services IoT offre des capacités en matière de gestion des dispositifs, de gestion des connexions, de fonctionnement des applications, d'analyse des activités, etc. Sur le plan de la gestion des données, la plate-forme de services IoT permet de recueillir, de stocker et de traiter des données (y compris les données personnelles et les informations confidentielles des utilisateurs) pour les applications IoT et pour procéder à des analyses évoluées.

4 Abréviations et acronymes

La présente Recommandation utilise les abréviations et acronymes suivants:

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

CSRF falsification de requête intersites (*cross site request forgery*)

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

DoS déni de service (*denial of service*)

IMEI	identité internationale d'équipement mobile (*international mobile equipment identity*)
PVLAN	réseau VLAN privé (*private VLAN*)
SIM	module d'identité de l'abonné (*subscriber identity module*)
SQL	langage de requête structuré (*structured query language*)
SSRF	falsification de requête côté serveur (*server side request forgery*)
VLAN	réseau local virtuel (*virtual local area network*)
VM	machine virtuelle (*virtual machine*)
VMM	hyperviseur (*virtual machine monitor*)
XSS	script intersites (*cross site script*)

5 Conventions

L'usage du conditionnel dans le présent document 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.

6 Aperçu général

La norme [ISO/CEI 30141] définit un modèle de référence de l'IoT basé sur une entité, comme indiqué dans la Figure 1. La plate-forme de services IoT est une composante essentielle du *sous-système d'applications et de services* représenté dans cette figure, lequel fournit des capacités notamment en matière de gestion des dispositifs, de gestion des connexions, de fonctionnement des applications et d'analyse des services. La plate-forme de services IoT réalise en outre des tâches de collecte, de stockage et d'analyse des données aux fins des applications IoT.

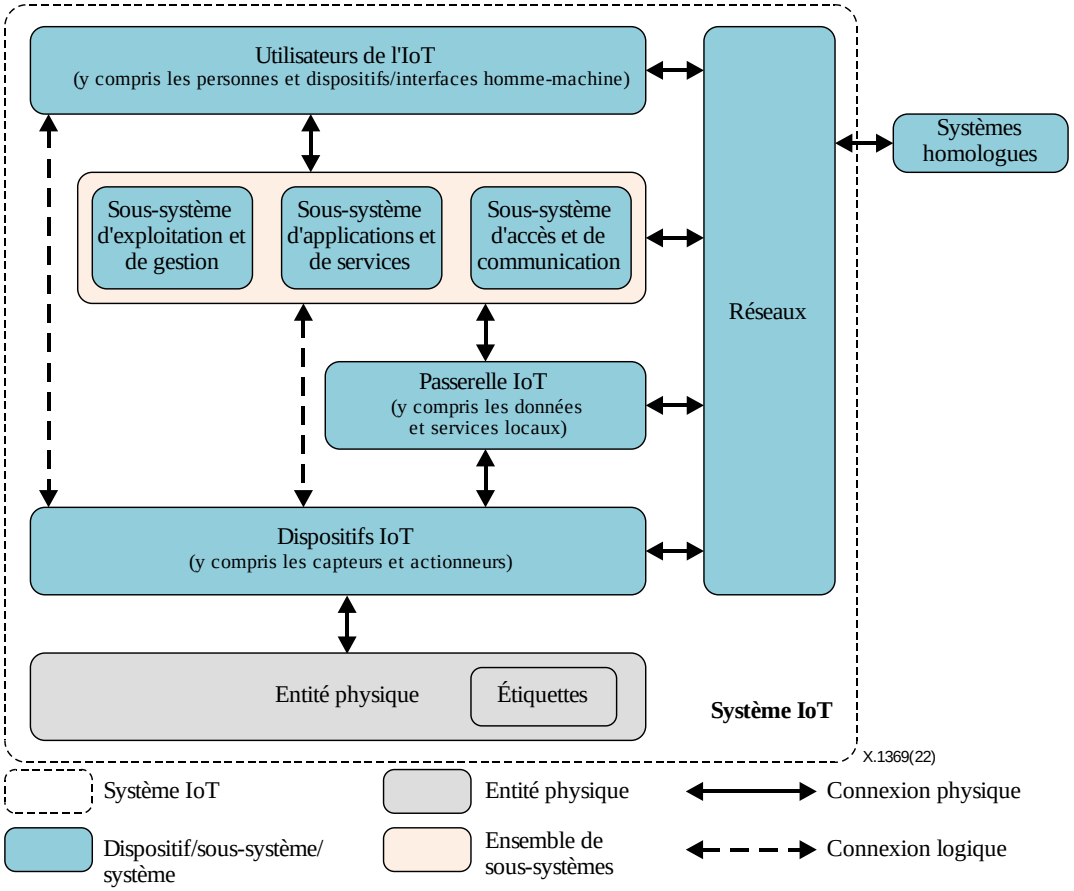

Figure 1 – Modèle de référence de l'IoT basé sur une entité [ISO/CEI 30141]

De manière générale, la plate-forme de services IoT peut être divisée en quatre parties, à savoir le système de gestion des dispositifs, le système de gestion de la connectivité, le système d'applications et le système d'analyse des activités.

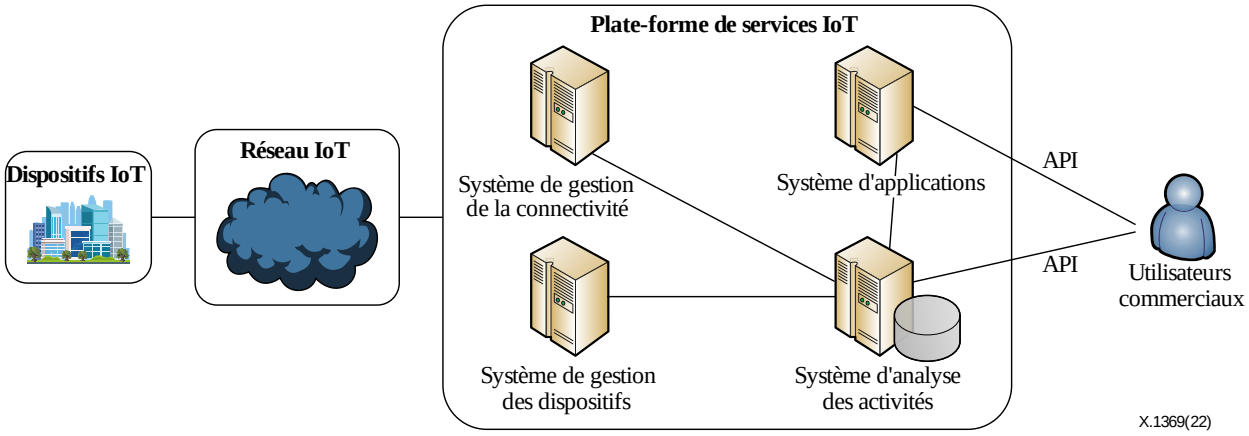

Figure 2 – Aperçu général de la plate-forme de services IoT

- Système de gestion des dispositifs

Il s'agit du système de gestion des dispositifs IoT, qui comprend notamment des fonctions de contrôle à distance, de reconfiguration, de mise à niveau des logiciels, de mise à niveau du système, de résolution des problèmes et de gestion du cycle de vie.

- Système de gestion de la connectivité

Il s'agit du système centralisé de gestion de la carte SIM (module d'identité de l'abonné). Ce système se concentre sur les applications des réseaux cellulaires et permet aux utilisateurs d'utiliser des services de manière autonome, notamment pour ce qui est d'envoyer des requêtes concernant l'utilisation des données et l'état de la connexion, de recharger la carte SIM et de gérer le trafic.

- Système d'applications

Il s'agit d'une plate-forme en tant que service qui fournit différentes fonctions de type interface de programmation d'application (API) pour mettre en œuvre divers systèmes de services. Un tel système permet aux opérateurs de télécommunication d'ouvrir leurs capacités de télécommunication essentielles (données, SMS, téléphonie, authentification, facturation, etc.) à divers systèmes de services, par exemple des systèmes de transports intelligents, de villes intelligentes, de maisons intelligentes, etc.

- Système d'analyse des activités

Il s'agit d'un système qui recueille diverses données auprès du système de gestion des dispositifs, du système de gestion de la connectivité et du système d'applications à des fins d'analyse et de production de comptes rendus visuels destinés aux opérateurs et aux consommateurs.

La sécurité de la plate-forme de services IoT joue un rôle important dans l'ensemble de l'environnement IoT. Toute faille ou attaque de la plate-forme aurait des conséquences pour la sécurité des dispositifs, des réseaux et des données connexes. La plate-forme de services IoT est vulnérable aux menaces liées notamment au déni de service (DoS), à l'élévation des privilèges, aux accès non autorisés, à la force brute, à l'exécution d'un code arbitraire, etc., ce qui peut conduire, entre autres conséquences graves, à des invasions malveillantes, à des fuites d'informations sensibles et à l'envoi d'instructions malveillantes à des dispositifs.

La présente Recommandation contient une analyse des risques auxquels les plates-formes de services IoT sont exposés sur le plan de la sécurité. Elle propose en outre un cadre et des mesures de sécurité.

La sécurité de la plate-forme de services IoT comprend la sécurité des infrastructures, la sécurité des systèmes, la sécurité des données et la sécurité des applications à tous les niveaux. La sécurité des interfaces API et la sécurité opérationnelle concerne les quatre niveaux. Dans les paragraphes 7 à 9, les risques de sécurité, le cadre de sécurité et les exigences de sécurité sont expliqués en détail eu égard à ces six aspects de la sécurité.

7 Menaces pour la sécurité de la plate-forme de services IoT

7.1 Menaces pour la sécurité des applications

Les menaces pour la sécurité des applications comprennent les attaques web, les accès non autorisés, l'élévation des privilèges et les vulnérabilités des services.

7.1.1 Attaques web

La plate-forme de services IoT utilise des technologies web traditionnelles et des technologies de communication, les mégadonnées, l'informatique en nuage, etc. Par conséquent, elle est exposée aux principaux risques de sécurité associés à toutes ces technologies tels que les attaques par déni de service réparti (DDoS), les attaques de type force brute, les injections de codes en langage de requête structuré (SQL) et les vulnérabilités résultant de l'exécution d'un script intersites (XSS), de la falsification de requête intersites (CSRF) ou de la falsification de requête côté serveur (SSRF), etc.

7.1.2 Accès non autorisés et élévation des privilèges

Bon nombre d'applications IoT sont déployées sur la plate-forme centralisée. Par conséquent, il est difficile d'assurer une isolation efficace en matière de sécurité et de contrôler les accès aux différentes applications, ce qui peut donner lieu à des accès et à une exploitation non autorisés et à l'élévation des privilèges. De plus, différents utilisateurs et dispositifs peuvent obtenir des accès non autorisés et une élévation des privilèges.

7.1.3 Vulnérabilités des services

Les applications IoT suivent une logique de service complexe et disposent d'un grand nombre de protocoles d'application, d'où de possibles failles dans leurs processus de conception et de mise en œuvre, pouvant engendrer des vulnérabilités et faire l'objet d'utilisations abusives. Dans certains scénarios d'applications de l'IoT, les terminaux peuvent être contrôlés grâce à la plate-forme. Toute plate-forme compromise mettrait inévitablement en péril un grand nombre de terminaux, ce qui aurait des répercussions sur les activités de production commerciale et la vie sociale des utilisateurs.

7.1.4 Exposition des capacités

En tant que plate-forme fournissant des applications, la plate-forme IoT peut proposer des interfaces API aux fonctions différentes pour contribuer à la mise en œuvre de différents systèmes de services. Si elle a pour effet d'accroître la commodité de divers services, l'ouverture des capacités peut aussi présenter des risques pour la plate-forme. Des développeurs non autorisés peuvent avoir accès à ces capacités, et différents services peuvent s'en servir de manière abusive. De plus, faute de protection appropriée, l'ouverture des capacités de télécommunication essentielles (données, SMS, téléphonie, authentification, facturation, etc.) peut exposer le réseau central de télécommunication à des attaques.

7.2 Risques pour la sécurité des données

La confidentialité, l'intégrité et la disponibilité des données constituent les fondements de la sécurité des données. Cependant, dans le cadre de la collecte, de la transmission, de la migration, du stockage, du traitement et de l'élimination des données, de nombreux risques existent.

7.2.1 Fuite de données

Les données des applications IoT sont généralement collectées par des terminaux IoT et transmises à la plate-forme, où elles sont normalement stockées. Faute de protection appropriée, une partie adverse peut donc mettre la main sur ces données grâce à des attaques par injection d'un code SQL, à une attaque par débordement de tampon, à une promotion des privilèges, etc.

7.2.2 Altération des données

Les données peuvent être altérées, reproduites ou modifiées pendant leur transmission. Dans le cadre de la transmission et du stockage des données des applications, une partie adverse peut, faute de protection appropriée, altérer des données. Elle peut par exemple reproduire des informations utilisées ou produire de fausses informations et les envoyer à la plate-forme IoT s'il n'est pas tenu compte de l'intégrité des données pendant la phase de transmission.

7.3 Risques pour la sécurité des systèmes

7.3.1 Compte compromis

Si les comptes des administrateurs de la plate-forme de services IoT du système d'exploitation ne sont pas suffisamment complexes, ou qu'un port superflu d'accès au système est ouvert, ces comptes peuvent être compromis au moyen d'attaques de type force brute, d'une surveillance, etc. L'inadéquation des contrôles d'accès est une menace pour la sécurité des systèmes.

7.3.2 Utilisation abusive des privilèges

Les services IoT fournis par la plate-forme fonctionnent grâce au système d'exploitation ou à l'intergiciel. Si le système d'exploitation ou l'intergiciel n'est pas mis à jour à temps, il y a des risques qu'une ancienne version du système ou de l'intergiciel présente des vulnérabilités susceptibles d'être exploitées par des pirates informatiques, ce qui pourrait conduire à une élévation des privilèges.

7.4 Risques pour la sécurité des infrastructures

Les infrastructures sont vulnérables à des menaces relatives à la sécurité physique, la sécurité du réseau, la sécurité virtuelle et la sécurité matérielle.

7.4.1 Menaces physiques

L'environnement physique de la plate-forme IoT a également des conséquences sur la sécurité. Il est par exemple vulnérable à des risques naturels tels que des tremblements de terre, des inondations, des tempêtes et des tornades. De plus, les installations, comme les systèmes d'alimentation électrique et de refroidissement, et même les systèmes de sécurité peuvent représenter une menace pour une plate-forme IoT. En outre, il conviendrait de tenir compte des facteurs humains, qui peuvent prendre la forme de destructions intentionnelles, de vols et d'explosions.

7.4.2 Menace relative au réseau

Les auteurs d'attaques peuvent explorer l'Internet pour trouver des points d'accès aux plates-formes de services IoT. Le manque d'isolation des réseaux de plates-formes de services peut permettre d'accéder à des données dans différents services.

7.4.3 Risques virtuels

Si les technologies de virtualisation des serveurs ont permis d'accroître considérablement l'efficacité de la construction de la plate-forme IoT, sa souplesse opérationnelle et ses avantages économiques, elles ont également fait apparaître de nouveaux risques. Les défauts de conception des hyperviseurs (VMM) permettent par exemple aux auteurs d'attaques de s'introduire sans autorisation dans un hôte virtuel OMTP, et le partage de la carte réseau avec la machine virtuelle du même hôte facilite la propagation des problèmes de sécurité. D'autres types de risques existent également, comme le passage d'une machine virtuelle à l'autre, les attaques DoS et la gestion à distance des vulnérabilités de la plate-forme.

7.5 Risques pour la sécurité de l'interface

L'interface de la plate-forme de services IoT comprend l'interface web, l'interface API tierce et l'interface API arrière du vendeur, lesquelles sont confrontées aux risques de fuite d'information, d'exécution d'un script intersites, d'une authentification faible et de contrôles d'accès faibles.

7.6 Risques pour la sécurité opérationnelle

Au cours de l'exploitation et de la maintenance, une mauvaise intervention du personnel chargé de ces tâches peut conduire à une interruption des services. Le personnel pourrait, par exemple, utiliser une clé USB infectée par un logiciel malveillant ou supprimer accidentellement des données. Il conviendrait aussi de tenir compte des connexions anormales, des mots de passe par défaut, des attaques malveillantes et des mécanismes d'audit.

8 Architecture de sécurité de la plate-forme de services IoT

L'architecture de sécurité de la plate-forme de services IoT est axée sur six aspects liés aux exigences de protection de la sécurité: la sécurité des applications, la sécurité de l'interface, la sécurité des données, la sécurité des systèmes, la sécurité des infrastructures et la sécurité opérationnelle.

L'architecture de sécurité globale est indiquée dans la Figure 3:

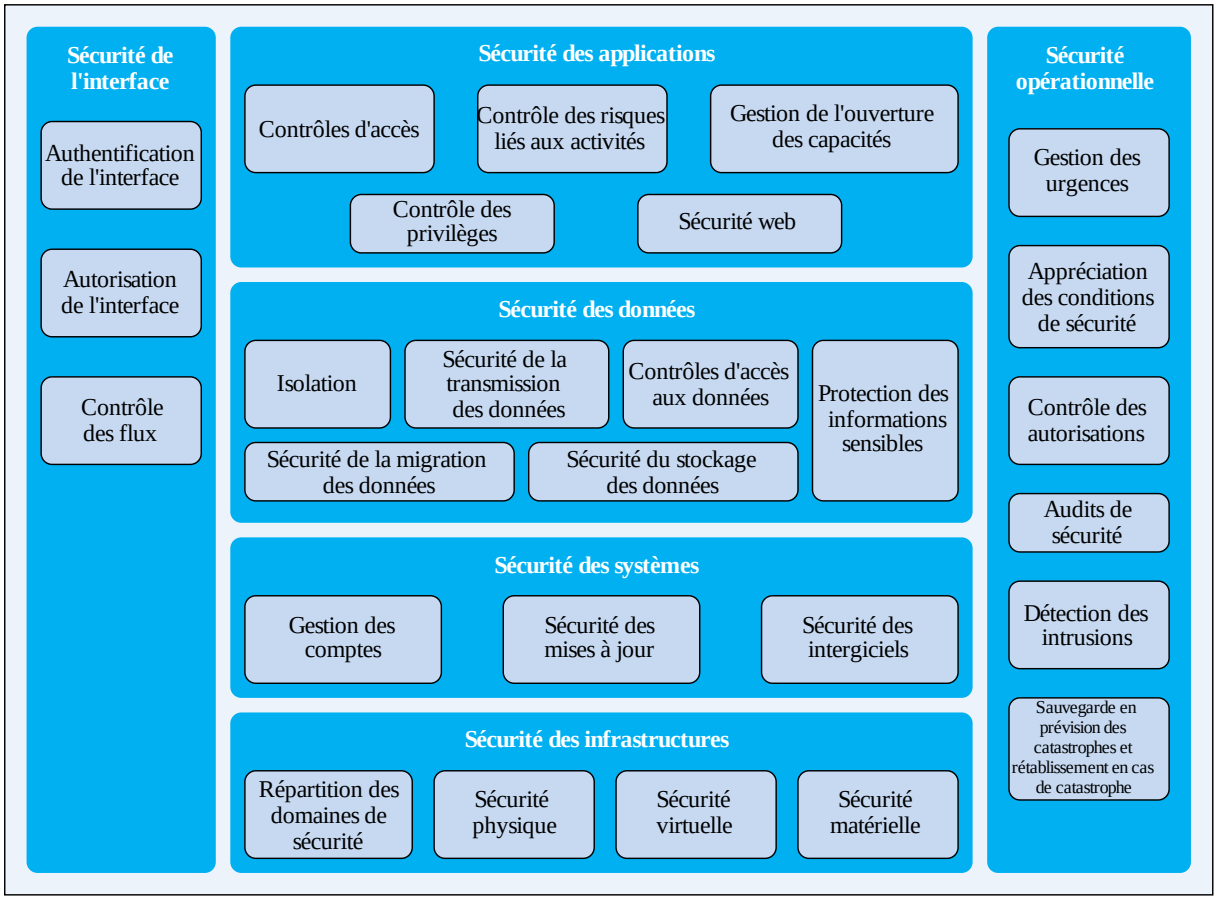

Figure 3 – Architecture de sécurité de la plate-forme de services IoT

8.1 Sécurité des applications

La sécurité des applications comprend les contrôles d'accès, le contrôle des privilèges, le contrôle des risques liés aux activités, la sécurité web et la gestion de l'exposition des capacités et pourrait permettre de résoudre les problèmes d'élévation des privilèges, d'accès non autorisés, etc.

8.2 Sécurité des données

La sécurité des données comprend l'isolation, la sécurité de la transmission des données, les contrôles d'accès et la sécurité du stockage des données et pourrait permettre de résoudre les problèmes liés aux fuites de données confidentielles, entre autres problèmes liés à la sécurité des données.

8.3 Sécurité des systèmes

La sécurité des systèmes comprend la gestion des comptes, la sécurité des mises à jour des logiciels et la sécurité des intergiciels et pourrait permettre de résoudre les problèmes liés aux utilisations malveillantes des vulnérabilités connues.

8.4 Sécurité des infrastructures

La sécurité des infrastructures comprend la répartition des domaines de sécurité, la sécurité physique, la sécurité virtuelle et la sécurité matérielle et pourrait permettre de résoudre les problèmes liés aux utilisations malveillantes des vulnérabilités connues.

8.5 Sécurité de l'interface

La sécurité de l'interface comprend l'authentification de l'interface, l'autorisation de l'interface et le contrôle des flux et pourrait permettre de résoudre les problèmes liés à la violation des informations d'identification personnelle, à l'injection d'un code SQL, etc.

8.6 Sécurité opérationnelle

La sécurité opérationnelle comprend la gestion des urgences, l'appréciation des conditions de sécurité, le contrôle des autorisations, les audits de sécurité, la détection des intrusions, la sauvegarde en prévision des catastrophes et le rétablissement en cas de catastrophe, ce qui pourrait permettre de résoudre des problèmes liés à la sécurité opérationnelle.

9 Exigences de sécurité pour la plate-forme de services IoT

9.1 Sécurité des applications

La plate-forme de services devrait être capable d'empêcher les attaques aux frontières lancées depuis l'Internet, en particulier celles qui visent les mégadonnées, l'informatique en nuage, les applications web et d'autres technologies. La capacité de prévenir les attaques DDoS, les altérations, les intrusions et les virus devrait être garantie pour que la plate-forme de services soit exploitée de façon sécurisée et stable.

9.1.1 Contrôles d'accès

9.1.1.1 Contrôles d'accès des utilisateurs

1) Un système d'identification des utilisateurs devrait être construit de telle sorte qu'il assigne un identifiant unique à chaque utilisateur, qui devrait rester le même y compris en cas de changement du numéro de téléphone, de la messagerie ou de toute autre information de l'utilisateur.
2) Les mots de passe faibles devraient faire l'objet d'une détection périodique. De plus, le mot de passe devrait être chiffré dans le cadre du processus de transmission. Pour les services nécessitant une sécurité élevée, il devrait être envisagé de mettre en place un mécanisme obligatoire de changement du mot de passe à intervalles réguliers.
3) L'utilisation de messages courts dynamiques devrait être rigoureusement encadrée. Des mesures de sécurité comme la vérification des antécédents, l'invalidation immédiate après utilisation, la limitation du nombre d'identifiants de connexion erronés, l'impossibilité de s'authentifier en local, etc., devraient être adoptées.
4) Un mécanisme de code d'authentification visuel devrait être utilisé dans le scénario de connexion. Il devrait être envisagé d'adopter des mesures d'embrouillage telles que le recours à un bruit de fond, la non-binarisation, la non-segmentation, la distorsion de la rotation des caractères, par ligne, etc., afin de prévenir la reconnaissance automatique rapide.
5) La plate-forme devrait permettre de maîtriser les risques et de prévenir les collisions. Elle devrait aussi permettre d'identifier les accès légitimes. Le cassage de mots de passe par la force devrait par exemple être évité moyennant la limitation du nombre d'échecs de connexion, les adresses IP, les identificateurs de dispositifs, les heures de verrouillage, le mode déverrouillage et les connexions simultanées.
6) Au cours du processus de redéfinition et de récupération du mot de passe, l'identité devrait faire l'objet d'une vérification rigoureuse pour qu'il soit impossible de contourner l'obligation d'authentification et éviter la contrefaçon d'identité.

9.1.1.2 Contrôles d'accès aux applications

1) Mettre en place un système d'identification des applications et attribuer un identifiant unique à chaque application.
2) La validité d'une application qui accède à la plate-forme devrait être authentifiée. Seule une application authentifiée devrait pouvoir accéder à la plate-forme de services pour invoquer des services.
3) Il est interdit de transférer des clés en clair ou de les transformer à l'aide d'un algorithme faible (par exemple MD5) au cours du processus d'authentification de l'application.
4) Différentes clés devraient être attribuées à différentes applications, et des fonctions de gestion des clés permettant de créer des clés, de les répartir, de les stocker et de les mettre à jour devraient être proposées.
5) Les invocations d'interfaces devraient faire l'objet d'une authentification pour limiter le champ des ressources et l'autorité opérationnelle qui peuvent être exploitées.

9.1.1.3 Contrôles d'accès aux dispositifs

1) Un système d'identification des dispositifs devrait être mis en place. Il s'agit d'attribuer à tous les dispositifs IoT un identifiant unique et d'associer cet identifiant aux informations de l'équipement correspondant, comme le fabricant du dispositif, le type de dispositif, son modèle, etc.
2) Attribuer une clé unique à chaque dispositif à l'aide d'un modèle de répartition préalable des clés ou encore d'un modèle d'échange de clés. La clé et l'identifiant du dispositif devraient être reliés. Des fonctions de gestion des clés permettant de créer des clés, de les répartir, de les stocker et de les mettre à jour devraient être proposées.
3) Procéder à l'authentification de l'identité lorsque le dispositif accède à la plate-forme. Seul un dispositif authentifié devrait pouvoir accéder à la plate-forme de services pour en exploiter les services.
4) Il est interdit de transférer des clés en clair ou de les transformer à l'aide d'un algorithme faible (par exemple MD5) au cours du processus d'authentification de l'application.

9.1.2 Contrôle des privilèges

1) Il devrait être possible de classer les utilisateurs et de gérer les groupes d'utilisateurs. Des privilèges différents devraient être accordés en fonction du classement et des groupes d'utilisateurs. Seuls les utilisateurs autorisés devraient pouvoir accéder à telles ou telles données et effectuer les tâches correspondantes.
2) Différents privilèges devraient être accordés en fonction des différentes classes d'applications. Seules les applications autorisées devraient pouvoir invoquer telles ou telles capacités de service et effectuer les tâches correspondantes.
3) Différents privilèges devraient être accordés en fonction des différents types ou des différentes classes de dispositifs. Seuls les dispositifs autorisés devraient pouvoir accéder à telles ou telles données ou informations et exécuter les tâches correspondantes.

9.1.3 Contrôle des risques liés aux activités

9.1.3.1 Gestion et contrôle de la sécurité des cartes IoT

Les fonctions de communication des cartes IoT devraient être rigoureusement limitées pour différents types de services sur la base "du minimum, du nécessaire et du contrôlable". Par exemple, pour la fonction vocale, les messages courts devraient être unidirectionnels dans certains scénarios, et la fonction de données devrait être restreinte lorsque le flux de données est anormal.

9.1.3.2 Gestion et contrôle de la sécurité des services

Il devrait être possible de limiter la quantité totale et la fréquence des flux de données, des messages courts, des communications vocales, etc., et d'interrompre le service en cas de dépassement du seuil.

9.1.3.3 Contrôle du comportement des utilisateurs

La quantité totale des flux, leur fréquence et la durée d'accès des utilisateurs à la plate-forme devraient être limitées. En cas de comportement anormal, l'accès devrait être immédiatement suspendu.

9.1.3.4 Surveillance des anomalies des dispositifs

Le comportement des dispositifs devrait faire l'objet d'une surveillance. Lorsqu'un comportement anormal (par exemple heure ou visite inhabituelles ou géolocalisation anormale) est détecté, un mécanisme d'alarme et de traitement devrait exister.

9.1.3.5 Suivi des risques liés aux services

Les données des terminaux IoT devraient faire l'objet d'une analyse à différents niveaux, notamment en ce qui concerne leur quantité totale et le débit de pointe, afin de déceler à temps toute anomalie dans le fonctionnement des services. Au cours de l'exploitation des services, toute utilisation abusive devrait également faire l'objet d'une surveillance. Une séparation du dispositif et de la carte peut par exemple être détectée au moyen d'une surveillance des numéros d'identité internationale d'équipement mobile (IMEI) des dispositifs. En même temps, l'utilisation des mégadonnées recueillies à partir de l'exploitation du terminal pourrait permettre, de manière générale, d'améliorer la capacité de détection, d'analyse et d'élimination des risques pour la sécurité.

9.1.4 Sécurité web

1) Une capacité robuste de lutte contre les attaques DDOS devrait être fournie, et les stratégies de lutte contre les attaques DDOS (par exemple traction du trafic, nettoyage du trafic réseau, etc.) applicables à la couche application et à la couche réseau devraient être spécialement adaptées.
2) La plate-forme devrait être dotée de capacités de recherche des vulnérabilités web, qui permettent de détecter et de prévenir les problèmes de sécurité tels que le téléchargement de fichiers, l'injection d'un code SQL, les vulnérabilités liées à un script XSS, les vulnérabilités liées à la falsification CSRF et les vulnérabilités liées à la falsification SSRF.
3) La plate-forme devrait permettre de rechercher les vulnérabilités de l'hôte et de trouver les vulnérabilités dans le système d'information, notamment les vulnérabilités en matière de sécurité, les problèmes de configuration des paramètres de sécurité, les vulnérabilités liées à la sécurité du système d'applications ainsi que les mots de passe faibles.
4) La plate-forme devrait permettre de limiter le temps de connexion à la base de données et d'accès au réseau dans les applications web afin d'éviter de consommer inutilement des ressources.
5) La plate-forme devrait permettre de détecter les intrusions, d'enregistrer l'adresse IP d'origine, le type d'attaque, le but et l'heure de celle-ci et prévoir un dispositif d'alarme en cas d'intrusion grave.

9.1.5 Gestion de l'exposition des capacités

9.1.5.1 Authentification de l'identité

Le système d'applications devrait permettre d'authentifier les identités. Lorsque le développeur demande et applique certaines fonctions d'interface API, la légalité du développeur et des applications devraient être authentifiées, et l'identité des développeurs et des applications légitimes ne devrait pas être usurpée.

9.1.5.2 Renforcement et protection des applications

Le système d'applications devrait permettre de renforcer et de protéger les applications qui invoquent les fonctions d'interface API, afin d'éviter qu'une application ne soit altérée ou décompilée.

9.1.5.3 Protection de la sécurité des données

Le système d'applications devrait garantir la confidentialité et l'intégrité des informations sensibles liées aux comptes, aux justificatifs des utilisateurs et aux applications, afin d'éviter le vol ou l'altération des informations pendant leur stockage, leur transmission et leur utilisation. Les informations sensibles transmises entre les applications IoT et la plate-forme devraient par exemple être chiffrées, et il conviendrait d'envisager de garantir leur intégrité, afin que ces informations ne soient pas dévoilées aux entités et processus non autorisés, et que ces entités et processus ne puissent les modifier, les fausser ou les reproduire, etc.

9.1.5.4 Authentification des invocations de capacités

Le système d'applications devrait permettre d'authentifier et d'autoriser les invocations de capacités. Lorsque l'application invoque des capacités, la fréquence, la quantité totale et le type de capacités que le développeur et l'application peuvent invoquer devraient être authentifiés. Les capacités ne devraient être invoquées qu'une fois l'autorisation accordée.

9.1.5.5 Suivi des invocations de capacités

Le système d'applications devrait permettre de suivre la fréquence, l'heure et la quantité totale des invocations de capacités. Lorsque la limite est dépassée ou le comportement est anormal, la fonction devrait être suspendue immédiatement et une alarme devrait être donnée au même moment.

9.2 Sécurité des données

La plate-forme devrait protéger les données tout au long de leur cycle de vie, notamment pendant leur stockage, leur transmission, leur utilisation, etc. Les données relatives aux services essentiels devraient être sauvegardées régulièrement, et un mécanisme de rétablissement devraient être mis en place, afin de garantir la confidentialité, l'intégrité et la disponibilité des données.

9.2.1 Isolation des données

Différentes données devraient être exécutées et sauvegardées dans des environnements isolés. La plate-forme devrait pouvoir isoler les informations sensibles de façon logique et contrôler rigoureusement les interactions entre les différents champs.

9.2.2 Sécurité de la transmission des données

1) Les informations sensibles transmises entre la plate-forme de services et les dispositifs IoT et d'autres plates-formes de services (notamment le mot de passe de l'administrateur de l'arrière-plan, le mot de passe de connexion au système d'exploitation, le mot de passe de connexion au dispositif réseau et les réponses de protection de ces mots de passe) devraient être protégées de manière confidentielle.
2) L'intégrité des informations sensibles échangées entre les plates-formes de services, les dispositifs IoT et d'autres plates-formes de services devrait être protégée.

9.2.3 Contrôles d'accès

La plate-forme devrait permettre de contrôler les accès: différentes politiques d'accès aux bases de données des différents systèmes de virtualisation devraient par exemple être mises en place afin que les utilisateurs n'aient accès qu'à la base de données autorisée du système de services correspondant et non aux données d'autres systèmes de services pour lesquels ils n'ont pas d'autorisation.

9.2.4 Sécurité du stockage de données

1) Les données devraient être classées selon leur importance, et différents mécanismes devraient être mis en place en fonction des catégories de données. Les données peu importantes peuvent par exemple être stockées en clair, tandis que la confidentialité des données importantes devrait être garantie.
2) La plate-forme devrait fournir un mécanisme sécurisé de stockage des clés. Les clés peuvent par exemple être stockées au sein du dispositif de chiffrement ou dans un proxy prévu à cet effet pour éviter toute fuite.
3) L'intégrité des données devrait être protégée et un mécanisme de détection de l'intégrité devrait être fourni pour les données particulièrement sensibles, afin que l'endommagement ou la perte de ces données puissent être détectés à temps. Les données particulièrement sensibles comprennent le nom d'utilisateur, le numéro de compte, etc.
4) La plate-forme devrait fournir un mécanisme complet de sauvegarde et de rétablissement des données. Si les données sont perdues ou détruites, le mécanisme de sauvegarde devrait être utilisé pour restaurer les données, afin qu'elles ne soient pas perdues à la suite d'un accident.
5) La plate-forme devrait permettre d'archiver toutes sortes de données et de fichiers et de nettoyer les données et fichiers temporaires de façon automatique et périodique.
6) L'espace de stockage des fichiers, répertoires et bases de données du système devrait être libéré ou redistribué, et il devrait être possible de le nettoyer complètement et définitivement.

9.3 Sécurité des systèmes

Le système utilisé par la plate-forme devrait tenir compte de la gestion des comptes, de la sécurité des mises à jour des logiciels et de la sécurité des intergiciels, ce qui pourrait permettre de résoudre les problèmes liés aux utilisations malveillantes des vulnérabilités connues.

9.3.1 Gestion des comptes

1) Le système de la plate-forme devrait automatiquement enregistrer les journaux système, tels que les informations sur la connexion des utilisateurs, les informations sur le fonctionnement, etc.
2) Les systèmes administrés à distance à l'aide du protocole HTTP devraient prendre en charge les protocoles de chiffrement tels que le protocole HTTPS.
3) Un système doté d'une interface à caractères devrait déconnecter automatiquement un utilisateur après un temps donné.
4) Le système devrait tenir compte des contrôles d'accès aux ressources de l'hôte, par exemple pour créer un modèle et définir une politique de sécurité appropriée et ainsi contrôler l'accès des différents profils d'utilisateurs aux ressources de l'hôte.

9.3.2 Sécurité des mises à jour des logiciels

1) La version et les correctifs de sécurité du système d'exploitation devraient être mis jour en temps utile.
2) Seuls les composants et les applications nécessaires devraient pouvoir être installés.
3) Le système devrait ouvrir uniquement les ports nécessaires et fermer les ports superflus.

9.3.3 Sécurité des intergiciels

1) La version et les correctifs de sécurité des intergiciels devraient être mis à jour en temps utile.
2) Les interfaces superflues des intergiciels devraient être désactivées afin d'éviter toute fuite d'information du système.
3) Le drapeau de l'intergiciel (le bandeau portant le nom/numéro de version du logiciel) devrait être protégé pour éviter toute fuite d'information du système.

9.4 Sécurité des infrastructures

La sécurité des infrastructures devrait tenir compte de la répartition des domaines de sécurité, de la sécurité physique, de la sécurité virtuelle et de la sécurité matérielle, ce qui pourrait permettre de résoudre les problèmes liés aux utilisations malveillantes des vulnérabilités connues.

9.4.1 Répartition des domaines de sécurité du réseau

1) Les domaines de sécurité devraient être divisés entre les plates-formes de services et l'Internet, entre les plates-formes de services et les systèmes d'appui interne, et entre les différents systèmes de services hébergés sur la plate-forme. Les limites des domaines de sécurité devraient mettre en place une séparation entre le domaine d'accès et les autres domaines, entre le domaine d'accès et le domaine central, et au sein même du domaine central.

2) Les différents systèmes de services de la plate-forme de services devraient être répartis en différents réseaux locaux virtuels (VLAN), et les différents domaines de sécurité devraient utiliser des segments VLAN différents. Les différents systèmes de services de chaque domaine de sécurité devraient utiliser des réseaux VLAN différents, tous les réseaux VLAN étant par défaut isolés. Au sein d'un réseau VLAN, il devrait être possible d'isoler les machines virtuelles en fonction des différents niveaux de sécurité d'un même système de services, par exemple en divisant un sous-réseau VLAN grâce à la technique des réseaux VLAN privés (PVLAN).

3) Une politique d'accès mutuel devrait être configurée. Il s'agit par exemple de configurer de manière stratégique les accès mutuels à différents domaines de sécurité au sein du système de services et les accès mutuels entre les différents systèmes de services.

4) Il devrait être possible d'isoler les domaines de sécurité. Le réseau de la plate-forme peut par exemple être divisé en un domaine de gestion, un domaine de services, un domaine d'interfaces, etc. Les dispositifs ayant des fonctions différentes devraient être répartis entre différents domaines de sécurité. Il conviendrait de détecter les intrusions et d'effectuer les contrôles d'accès aux frontières entre les domaines de sécurité.

9.4.2 Sécurité physique

1) L'environnement physique devrait satisfaire aux exigences de protection de la sécurité pour ce qui est de l'emplacement, de l'alimentation électrique, des incendies, de la résistance à l'eau, de la prévention des décharges d'électricité statique et de la maîtrise de la température et de l'humidité.

9.4.3 Sécurité virtuelle

1) La plate-forme devrait permettre, entre autres fonctions, de protéger les hyperviseurs, d'isoler les machines virtuelles, de renforcer le système d'hébergement en nuage, de surveiller la sécurité des machines virtuelles, de se protéger contre les logiciels malveillants et de contrôler les applications, afin d'éviter les problèmes de sécurité courants liés à la virtualisation.

9.4.4 Sécurité matérielle

1) Les installations matérielles devraient satisfaire aux exigences fondamentales de configuration en matière de protection de la sécurité et aux exigences de test. Des services informatiques de confiance devraient être proposés afin d'améliorer la sécurité des installations.

9.5 Sécurité de l'interface

La sécurité de l'interface comprend l'authentification de l'interface, l'autorisation de l'interface et le contrôle des flux et pourrait permettre de résoudre les problèmes liés à la violation des informations d'identification personnelle, à l'injection d'un code SQL, etc.

9.5.1 Authentification de l'interface

1) La plate-forme devrait permettre de vérifier la légitimité entre les systèmes de services, afin d'empêcher les recours et les accès non autorisés à la plate-forme.

2) La plate-forme de services devrait permettre d'enregistrer la totalité du journal d'exploitation des ressources invoquées.

9.5.2 Autorisation de l'interface

1) La plate-forme de services devrait permettre d'octroyer des autorisations en fonction de la plage d'adresses IP d'origine. En plus de fournir un mot de passe statique, la plate-forme de services invoquée doit aussi autoriser la plage d'adresses IP.

2) Les interfaces nécessitant des droits d'accès pour les utilisateurs devraient être dotées d'un mécanisme d'accès permettant de refuser/d'autoriser des listes afin d'intercepter les accès par des utilisateurs non autorisés.

9.5.3 Contrôle des flux

1) La plate-forme devrait permettre de contrôler le débit de flux en définissant la politique de contrôle des flux, la valeur configurée dans la politique pouvant être modifiée en fonction de l'évolution du fonctionnement du serveur de l'interface API d'arrière-plan. Lorsque le nombre de requêtes simultanées dépasse la limite fixée, les requêtes excédentaires sont rejetées et un message d'erreur est envoyé.

9.6 Sécurité opérationnelle

La sécurité opérationnelle comprend la gestion des urgences, l'appréciation des conditions de sécurité, le contrôle des autorisations, les audits de sécurité, la détection des intrusions, la sauvegarde en prévision des catastrophes et le rétablissement en cas de catastrophe, ce qui pourrait permettre de résoudre les problèmes liés à la sécurité opérationnelle.

9.6.1 Gestion des urgences

1) La plate-forme devrait créer un mécanisme d'intervention en cas d'urgence, par exemple en cas d'incident de cybersécurité, d'incident lié à la sécurité au travail, etc.

2) Il s'agit d'organiser régulièrement des exercices d'intervention en cas d'urgence et de mettre en place un système de planification régulière des exercices de ce type.

9.6.2 Appréciation des conditions de sécurité

1) Il est recommandé de mettre au point un système d'appréciation des conditions de sécurité pour surveiller, évaluer et visualiser les conditions de sécurité de la plate-forme, envoyer des alertes précoces et centraliser les interventions, l'objectif étant d'améliorer véritablement le suivi des menaces pour la sécurité du réseau, l'appréciation de la situation, les interventions en cas d'urgence et le traçage, entre autres capacités, et d'accroître l'efficacité du fonctionnement et du maintien du dispositif de sécurité.

9.6.3 Contrôle des autorisations

1) La plate-forme devrait prévoir les authentifications et autorisations nécessaires pour ses différentes opérations. Pour ce qui est des privilèges élevés, seul le personnel de confiance intervenant dans le système est autorisé à réaliser les opérations nécessitant des privilèges élevés.

2) La plate-forme devrait créer des modèles et contrôler les accès des utilisateurs aux ressources de l'hôte en fonction des politiques de sécurité.

9.6.4 Audit de sécurité

1) Toutes les activités des administrateurs devraient être enregistrées et consignées dans un journal.

2) Lorsque l'espace de stockage est presque saturé, il conviendrait de garantir que le journal d'audit ne soit pas perdu.

3) Les journaux d'audit devraient être sauvegardés.

4) Les journaux d'audit devraient être protégés contre les accès, les modifications ou les destructions sans autorisation.

5) Les journaux d'audit devraient être exportés et supprimés.

6) L'accès aux journaux devrait être sécurisé afin de garantir la confidentialité et l'intégrité du processus de transmission.

7) La plate-forme devrait permettre de surveiller en temps réel et de vérifier périodiquement les comportements anormaux tels que les connexions anormales, les accès anormaux et les applications anormales à partir d'analyses du trafic, de vérifications des journaux, de bacs à sable, etc., et les comportements anormaux avérés devraient donner lieu à des alertes et des suppressions sans délai.

9.6.5 Détection des intrusions

1) La plate-forme devrait déployer un dispositif de détection des intrusions afin de détecter rapidement toute intrusion.

9.6.6 Sauvegarde en prévision des catastrophes et rétablissement en cas de catastrophe

1) En cas d'incendie, de tremblement de terre ou de toute autre catastrophe, la plate-forme devrait pouvoir activer le système redondant de sauvegarde à distance suffisamment tôt pour éviter une interruption de service.

2) En cas de catastrophe, la plate-forme devrait permettre de rétablir les données sensibles (telles que les données de service, les données de facturation, les données de configuration du système, les données sur les activités des administrateurs et la maintenance, les informations relatives aux utilisateurs, etc.), afin de garantir que, en cas de suppression des données essentielles à des fins malveillantes, le système puisse être rétabli rapidement.

Bibliographie

[b-UIT-T X.1361] Recommandation UIT-T X.1361 (2018), *Cadre de sécurité applicable à l'Internet des objets fondé sur le modèle passerelle*.

[b-UIT-T X.1362] Recommandation UIT-T X.1362 (2017), *Procédure de chiffrement simple pour les environnements de l'Internet des objets (IoT).*

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

[b-UIT-T Y.4000] Recommandation UIT-T Y.4000/Y.2060 (2012), *Présentation générale de l'Internet des objets.*

[b-UIT-T Y.4100] Recommandation UIT-T Y.4100/Y.2066 (2014), *Exigences communes relatives à l'Internet des objets*.

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, 2022