Union internationale des télécommunications

UIT-T

SECTEUR DE LA NORMALISATION
DES TÉLÉCOMMUNICATIONS
DE L'UIT

X.1209

(12/2010)

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

Sécurité du cyberespace – Cybersécurité

Les capacités et leurs scénarios contextuels pour le partage et l'échange d'informations concernant la cybersécurité

Recommandation UIT-T X.1209

RECOMMANDATIONS UIT-T DE LA SÉRIE X

RÉSEAUX DE DONNÉES, COMMUNICATION ENTRE SYSTÈMES OUVERTS ET SÉCURITÉ

RÉSEAUX PUBLICS DE DONNÉES	X.1–X.199
INTERCONNEXION DES SYSTÈMES OUVERTS	X.200–X.299
INTERFONCTIONNEMENT DES RÉSEAUX	X.300–X.399
SYSTÈMES DE MESSAGERIE	X.400–X.499
ANNUAIRE	X.500–X.599
RÉSEAUTAGE OSI ET ASPECTS SYSTÈMES	X.600–X.699
GESTION OSI	X.700–X.799
SÉCURITÉ	X.800–X.849
APPLICATIONS OSI	X.850–X.899
TRAITEMENT RÉPARTI OUVERT	X.900–X.999
SÉCURITÉ DE L'INFORMATION ET DES RÉSEAUX	
Aspects généraux de la sécurité	X.1000–X.1029
Sécurité des réseaux	X.1030–X.1049
Gestion de la sécurité	X.1050–X.1069
Télébiométrie	X.1080–X.1099
APPLICATIONS ET SERVICES SÉCURISÉS	
Sécurité en multidiffusion	X.1100–X.1109
Sécurité des réseaux domestiques	X.1110–X.1119
Sécurité des télécommunications mobiles	X.1120–X.1139
Sécurité de la toile	X.1140–X.1149
Protocoles de sécurité	X.1150–X.1159
Sécurité d'homologue à homologue	X.1160–X.1169
Sécurité des identificateurs en réseau	X.1170–X.1179
Sécurité de la télévision par réseau IP	X.1180–X.1199
SÉCURITÉ DU CYBERESPACE	
Cybersécurité	**X.1200–X.1229**
Lutte contre le pollupostage	X.1230–X.1249
Gestion des identités	X.1250–X.1279
APPLICATIONS ET SERVICES SÉCURISÉS	
Communications d'urgence	X.1300–X.1309
Sécurité des réseaux de capteurs ubiquitaires	X.1310–X.1339
ECHANGE D'INFORMATIONS SUR LA CYBERSÉCURITÉ	
Aperçu général de la cybersécurité	X.1500–X.1519
Echange concernant les vulnérabilités/les états	X.1520–X.1539
Echange concernant les événements/les incidents/l'heuristique	X.1540–X.1549
Echange de politiques	X.1550–X.1559
Heuristique et demande d'informations	X.1560–X.1569
Identification et découverte	X.1570–X.1579
Echange garanti	X.1580–X.1589

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

Recommandation UIT-T X.1209

Les capacités et leurs scénarios contextuels pour le partage et l'échange d'informations concernant la cybersécurité

Résumé

La Recommandation UIT-T X.1209 décrit des scénarios de haut niveau et les capacités de prise en charge du partage et de l'échange d'informations concernant la cybersécurité. Cette Recommandation fournit les capacités importantes pour prendre en charge l'interopérabilité entre applications pour le partage et l'échange des informations concernant la cybersécurité.

Les capacités sont décrites et peuvent être utilisées dans des situations/scénarios prenant en charge des entités auparavant indépendantes, afin de participer à divers efforts coordonnés tels que la prévention ou l'arrêt des comportements cibles, ou la coordination des efforts d'analyse et de détermination.

L'objectif des capacités listées et décrites est de prendre en charge des opérations de sécurité plus efficientes et efficaces en prenant en charge le partage et l'échange interopérables d'informations entre les parties de confiance travaillant ensemble pour surveiller, maintenir et plus généralement gérer la sécurité des systèmes et réseaux.

Historique

Edition	Recommandation	Approbation	Commission d'études
1.0	ITU-T X.1209	2010-12-17	17

Mots clés

Echange d'informations, informations de cybersécurité, partage d'informations.

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.1209

Les capacités et leurs scénarios contextuels pour le partage et l'échange d'informations concernant la cybersécurité

1 Domaine d'application

Cette Recommandation fournit les capacités importantes pour la prise en charge de l'interopérabilité entre applications pour le partage et l'échange des informations concernant la cybersécurité. En conséquence, le § 7 contient les descriptions haut niveau des scénarios d'utilisation des capacités, qui sont utilisés pour fixer le contexte des capacités trouvées dans le § 8. Pour clarifier davantage l'objectif des capacités, le § 9 contient les descriptions des capacités les plus probablement nécessaires selon les situations.

Le public visé par cette Recommandation est constitué par les personnes impliquées dans les opérations de sécurité autorisées.

2 Références

Sans objet.

3 Définitions

3.1 Termes définis ailleurs

La présente Recommandation utilise le terme suivant défini ailleurs:

3.1.1 cybersécurité [b-ITU-T X.1205]: ensemble des outils, politiques, concepts de sécurité, mécanismes de sécurité, lignes directrices, méthodes de gestion des risques, actions, formations, bonnes pratiques, garanties et technologies qui peuvent être utilisés pour protéger le cyberenvironnement et les actifs des organisations et des utilisateurs. Les actifs des organisations et des utilisateurs comprennent les dispositifs informatiques connectés, le personnel, l'infrastructure, les applications, les services, les systèmes de télécommunication, et la totalité des informations transmises et/ou stockées dans le cyberenvironnement. La cybersécurité cherche à garantir que les propriétés de sécurité des actifs des organisations et des utilisateurs sont assurées et maintenues par rapport aux risques affectant la sécurité dans le cyberenvironnement. Les objectifs généraux en matière de sécurité sont les suivants:

- disponibilité;
- intégrité, qui peut englober l'authenticité et la non-répudiation;
- confidentialité.

3.2 Termes définis dans la présente Recommandation

Le terme suivant est défini dans la présente Recommandation:

3.2.1 informations concernant la cybersécurité: information ou connaissance structurée pouvant inclure, mais n'étant pas limitée à: "l'état" de l'équipement, du logiciel ou des systèmes réseaux; argumentation en relation avec des incidents ou événements; parties implémentant les capacités d'échange d'informations en termes de cybersécurité; spécifications pour l'échange d'informations en termes de cybersécurité, y compris les modules, schémas et numéros attribués; identités et attributs fiables pour tous les éléments précédents et prescriptions, lignes directrices et pratiques d'implémentation.

4 Abréviations et acronymes

La présente Recommandation utilise les abréviations et acronymes suivants:

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

FTP protocole de transfert de fichier (*file transfer protocol*)

HTTP protocole de transfert hypertexte (*hypertext transfer protocol*)

HTTPS protocole de transfert hypertexte sécurisé (*secure hypertext transfer protocol*) (HTTP sur SSL)

IPS système de prévention d'intrusion (*intrusion prevention system*)

5 Conventions

Sans objet.

6 Introduction

Les cyberattaques impliquant des virus, des vers, etc. réduisent leur vitesse de propagation au sein des réseaux en utilisant différentes techniques, évoluant toujours vers des formes plus menaçantes. Différents types de solutions de sécurité incluant des antivirus, des détections de logiciels espions, pare-feu, réseau privé virtuel, détection et protection contre les intrusions, etc. ont été développés, afin que les incidents de sécurité liés à de telles attaques menaçantes puissent être contrés par un système répondant rapidement en prenant des contre-mesures efficaces.

Pour les gestionnaires de sécurité, la ligne de défense la plus commune contre les exploits, virus, vers et botnets s'est tout d'abord trouvée dans les divers forums de discussion auxquels de nombreux professionnels de la sécurité sont abonnés. En général, en quelques jours à une semaine, les trous sont comblés, les vulnérabilités sont corrigées et les choses reviennent à la normale.

Malheureusement, l'exploitation des vulnérabilités par les virus, vers et botnets peut se propager très rapidement à travers le réseau. En quelques secondes, des réseaux entiers peuvent être touchés de manière significative.

L'échange d'informations concernant la cybersécurité au sein d'une organisation donnée peut se produire très rapidement. Cependant, l'échange d'un grand nombre d'informations entre organisations n'est pas bien pris en charge par les méthodes actuelles. L'absence de moyens de communication efficaces peut transformer chaque organisation en un îlot de sécurité.

C'est pourquoi il est important de partager les informations concernant la cybersécurité entre organisations, y compris les opérateurs de télécommunication, les fournisseurs de services de télécommunication et les centres d'opérations de sécurité. Pour rendre possible un tel échange d'informations, il est nécessaire d'avoir:

- des méthodes fiables et sûres pour que les participants échangent les informations plus rapidement;
- des méthodes pour s'assurer de la protection du secret des communications.

Cette Recommandation fournit les scénarios considérés et les capacités de prise en charge pour l'échange des informations de cybersécurité entre participants de manière sûre, solide et fiable.

7 Scénarios des capacités

Pour pouvoir mettre les capacités listées dans le § 8 dans le contexte approprié afin de comprendre cette Recommandation, des scénarios d'utilisation de haut niveau sont présentés dans cinq configurations différentes pour aider à expliquer les cinq groupes logiques de capacités suivants.

7.1 Scénario général

Ce scénario général s'applique à tous les scénarios subséquents.

Scénario: Les partenaires d'échange d'information partagent les informations utiles, liées à un événement ou à un incident concernant la sécurité, pour identifier et prévenir les attaques adverses sur leur réseau respectif.

L'aspect important de ce scénario est que les deux parties peuvent rassembler des données similaires, mais de sources différentes et/ou dans des formats différents et/ou de contenu légèrement différent pour des types de données similaires.

7.2 Politiques opérationnelles

Ce scénario décrit une situation dans laquelle les différents partenaires d'échange d'information ont des restrictions différentes quant à l'accès aux différents éléments des informations partagées.

Scénario: Les partenaires d'échange d'information ont un accord commercial pour partager les informations liées à un événement ou à un incident concernant la sécurité

Un aspect important de ce scénario est que l'accès aux informations de chaque partenaire d'échange peut être restreint avec un accès accordé sur la base d'une relation de confiance pré-existante. Un autre aspect important est que la confiance accordée à l'information reçue peut être associée à la relation de confiance qui existe.

7.3 Politiques régionales

Ce scénario décrit une situation où il existe de multiples partenaires d'échange d'information dans laquelle les partenaires respectifs ont différentes restrictions légales et/ou réglementaires sur un même type d'information partagée. De façon similaire au précédent scénario, ce scénario met également en lumière la possibilité qu'une personne puisse être autorisée à partager des informations auxquelles elle-même n'est pas autorisée à accéder ou qu'elle ne peut visualiser.

Ce scénario diffère du précédent du fait de la source des restrictions placées sur les échanges d'informations. La source des restrictions dans le précédent scénario est les politiques opérationnelles décidées par chaque partenaire d'échange d'information, tandis que les restrictions dans ce scénario sont dues aux politiques opérationnelles imposées par l'extérieur, telles que les juridictions régionales.

Scénario: Deux parties opérant dans différentes régions peuvent échanger des informations avec des prescriptions différentes sur ces informations imposées par les régions respectives.

L'aspect important de ce scénario est qu'en plus des parties ayant des politiques opérationnelles différentes, il peut également y avoir des politiques associées à la région dans laquelle les informations sont échangées.

7.4 Format d'échange

Scénario: Un partenaire d'échange d'information livre des informations, qui comprennent les ports et intervalles de ports impliqués, à un deuxième partenaire concernant un schéma de trafic gênant. Les informations partagées sont utilisées afin d'identifier les instances d'une attaque spécifique.

L'aspect important de ce scénario est que le contenu des informations échangées doit être facilement compris et en accord avec tous les partenaires d'échange d'information impliqués.

7.5 Protection de la vie privée

Les scénarios inclus dans ce paragraphe mettent en lumière différents problèmes liés à la vie privée, que la "vie privée" soit professionnelle ou personnelle. De plus, ils soulignent le besoin de pouvoir assurer le secret des échanges d'information eux-mêmes.

- Scénario: Un centre d'opérations de sécurité rassemble les informations liées à une attaque malveillante contre l'un des réseaux, systèmes et plus généralement l'un des biens qu'il gère. Ces informations sont alors fournies à un fournisseur de service de réseau pour identifier la ou les sources de l'attaque malveillante donnée.

  L'aspect important de ce scénario est que le fournisseur de service de réseau a la possibilité d'identifier personnellement la ou les sources suspectées de l'attaque, mais n'a pas besoin de divulguer l'information au centre d'opérations de sécurité.
- Scénario: L'ensemble complet des informations rassemblées par un partenaire d'échange d'information peut contenir des éléments que le partenaire d'échange d'information peut souhaiter révéler aux partenaires d'échange au sein de leur organisation ou des opérations, mais qu'il ne souhaitent pas révéler à ceux qui sont extérieurs à leurs opérations.

  L'aspect important de ce scénario est que les parties impliquées dans l'échange d'informations peuvent choisir de partager toutes les informations disponibles ou seulement un sous-ensemble, ou occulter d'une certaine manière tout ou partie des informations qu'elles partagent.
- Scénario: Deux parties échangent des informations sensibles sur des réseaux "publics".

  L'aspect important de ce scénario est que le secret des informations échangées doit pouvoir être assuré quelle que soit la méthode de communication utilisée.

7.6 Granularité de l'accès

Ce scénario met en lumière la situation dans laquelle différents types ou éléments d'informations concernant la sécurité peuvent être partagés sous et selon différentes conditions.

Scénario: Un service publie des avis et avertissements à la fois de manière gratuite et sous abonnement livrant différents niveaux d'information dépendant de la définition de services d'un abonnement donné.

Un exemple de différences entre niveaux peut être la mise à disposition de données brutes uniquement à un niveau, tandis qu'à un autre niveau les données brutes et analyses sont rendues disponibles.

L'aspect important de ce scénario est que bien que toutes les informations disponibles puissent être d'un type donné, il peut exister différents "niveaux" d'information rendus disponibles à d'autres tiers.

7.7 Vérification des sources

Ce scénario met en lumière le besoin d'authentification des partenaires d'échange d'information.

Scénario: Un partenaire d'échange d'information reçoit des informations d'un second partenaire et vérifie que les informations proviennent effectivement du second partenaire.

L'aspect important de ce scénario est que les parties échangeant des informations les unes avec les autres doivent vérifier que les informations provenaient bien de l'expéditeur prévu et non d'un tiers tentant de se faire passer pour l'expéditeur prévu.

7.8 Distribution multicanaux

Ce scénario, bien que similaire à "Granularité de l'accès", met en lumière la situation dans laquelle différents niveaux d'information peuvent être mis à disposition à l'aide de différentes méthodes.

Scénario: Un partenaire d'échange d'information rend des notifications et des alertes de sécurité disponibles par différents moyens et sous différentes conditions. Les données peuvent être disponibles pour téléchargement à partir d'un répertoire trouvable gratuitement, fourni

sélectivement par courriel pour un niveau de service, ou disponible sous une forme lisible et accessible par une machine pour un autre niveau de service.

L'aspect important de ce scénario est que des informations identiques ou différentes peuvent être mises à disposition via un grand nombre de moyens et sous un grand nombre de conditions.

7.9 Compatibilité avec les versions antérieures

Scénario: Deux partenaires d'échange d'information ont déjà échangé des informations spécifiques à l'aide de formats et protocoles spécifiques. Une nouvelle norme prenant en charge leur méthode d'échange actuelle devient disponible et fournit de nouvelles fonctionnalités supplémentaires.

Il importe dans ce scénario de prendre en charge les applications existantes, autant que possible, tout en leur fournissant une procédure de mise à niveau pour peu que de nouvelles normes deviennent disponibles.

8 Capacités

Les paragraphes suivants listent les différentes capacités prenant en charge les types de scénarios listés ci-dessus dans le § 7.

8.1 Capacités de format/encodage

- Le format et la structure des informations concernant la sécurité doivent être connus et compris par les deux parties.
  - Les informations échangées concernant la sécurité sont de nature hétérogène, tels que des messages et signatures d'un pare-feu ou de tout autre appareil de sécurité de réseau, ainsi que différents types d'informations spécifiques à l'application, tels que des rapports, analyses, réponses, et échanges de données d'argumentation en relation avec des incidents ou événements
  - Le format des informations échangées représente différents types d'informations concernant la sécurité générés par et applicables à des environnements systèmes hétérogènes
- Divers types d'informations liées à la sécurité doivent pouvoir être partagés. Les exemples comprennent, mais ne sont pas limités aux signatures de comportement de trafic, aux signatures d'accès au système, aux adresses IP source, aux intervalles de ports source et/ou destination, etc.
- Les parties doivent pouvoir être capables d'inclure différents niveaux d'information, du contenu d'un unique paquet, à tous les paquets impliqués dans une attaque DDoS sur le réseau entier.
- Le contenu des informations concernant la sécurité doit être connu et compris des deux parties.
- Le sujet, la possibilité d'utilisation et d'application des informations doivent être identifiables.

8.2 Capacités de transfert/échange

- Les parties doivent pouvoir transférer, livrer et recevoir des informations concernant la sécurité au travers d'une gamme large et extensible de distributions et de médiums de transmission.
- Les applications peuvent devoir prendre en charge les échanges synchrones et asynchrones entre les parties au cours du partage et de l'échange d'informations concernant la sécurité.
- Les applications peuvent devoir la livraison d'informations sur un mode d'envoi (*push*), de réception (*pull*) ou par un abonnement.

- Les applications doivent prendre en charge des opérations stables au cours de l'échange et le traitement d'un grand nombre d'informations concernant la sécurité.
- Les protocoles d'échange utilisés doivent utiliser et/ou s'appuyer sur des protocoles existants déjà largement utilisés.

8.3 Capacités de sécurité

- Les informations concernant la cybersécurité impliquées dans le partage et l'échange doivent pouvoir être authentifiées et vérifiées.
- Les applications doivent prendre en charge la fiabilité, la confidentialité, l'intégrité et la disponibilité des informations et services.
- Les parties impliquées doivent être identifiables de manière authentifiée et vérifiable.
- Les applications doivent empêcher les attaques contre le partage et l'échange d'informations concernant la cybersécurité dues à l'invention et/ou la falsification des informations contenues ou de la source/destination des informations contenues.
- Les parties sources doivent pouvoir assurer que seules les parties autorisées peuvent accéder aux informations sensibles. Il s'agit d'assurer la confidentialité des communications et s'applique que le secret soit requis pour des informations identifiables personnellement ou pour des informations professionnelles privées, ou pour tout ce dont il est considéré comme important que cela reste privé et accessible uniquement aux personnes autorisées.
- Les parties sources doivent pouvoir contrôler l'accès à un niveau de granularité tel que seules les parties autorisées à accéder à des éléments spécifiques d'une information de sécurité donnée peuvent le faire et ne pas accéder à des éléments auxquels elles ne sont pas autorisées.
- Les parties doivent pouvoir sécuriser les informations liées à la sécurité contre tout accès par des parties non autorisées, même dans un environnement ouvert où les informations concernant la sécurité sont disponibles à tous, y compris aux parties non autorisées.

8.4 Capacités de politique

- Les parties doivent pouvoir définir et déclarer individuellement une politique applicable, localement et/ou sur le plan régional, en ce qui concerne l'approvisionnement et/ou l'accès aux informations de cybersécurité fournies.
- Les parties doivent pouvoir fournir et accéder aux informations concernant la sécurité d'une manière cohérente avec leurs politiques applicables respectives relativement à l'approvisionnement et/ou l'accès aux informations de sécurité.
- Les parties doivent pouvoir déclarer au sein de quelle juridiction un ensemble de déclarations de politique s'applique.
- Les parties doivent pouvoir définir et déclarer individuellement les prescriptions et limitations juridictionnelles possibles relativement à l'approvisionnement et/ou l'accès aux informations de sécurité au sein de leurs juridictions respectives.
- Les parties doivent pouvoir fournir et accéder aux informations de sécurité d'une manière cohérente avec les prescriptions juridictionnelles respectives.

8.5 Capacités de neutralité par rapport au vendeur

Afin de prendre en charge le partage et l'échange d'une gamme d'informations de cybersécurité aussi grande que possible, les applications doivent fournir des services ayant aussi peu de dépendance que possible envers un système spécifique à un vendeur ou des données spécifiques à un vendeur. En même temps, il est préférable également qu'aucun système ou donnée spécifique à un vendeur soit exclu.

9 Applicabilité des capacités

Les scénarios et capacités décrits dans cette Recommandation fournissent un ensemble "d'outils" discrets que l'on peut choisir de mélanger et de faire correspondre à son utilisation pour créer son application. Certaines applications moins complexes, telles que l'agrégation de données simples et/ou la recherche d'informations, peuvent ne nécessiter que quelques-unes des capacités listées, tandis que d'autres, qui sont riches en fonctions et fournissent de plus nombreux services, peuvent nécessiter de combiner et d'implémenter plusieurs des capacités.

Ce qui suit est une discussion concernant les moments pour lesquels des types spécifiques de capacités peuvent être plus nécessaires et ceux auxquels ils peuvent être de nature plus optionnelle.

9.1 Capacités de format/encodage

Pour que le moindre partage et échange d'informations de cybersécurité ait lieu, à la fois l'expéditeur et le destinataire doivent pouvoir comprendre exactement quel est le contenu de ce qu'ils échangent. Par conséquent, les capacités de format et d'encodage s'appliquent à chacun des scénarios au sein desquels les informations de cybersécurité sont partagées et/ou échangées.

9.2 Capacités de transfert/échange

De manière comparable à l'importance des capacités de format et d'encodage, deux ou plusieurs partenaires d'échange d'information ont besoin d'une méthode pour obtenir les informations de la part du côté expéditeur vers le côté destinataire.

9.3 Capacités de sécurité

Il ne sert que très peu d'échanger des informations relatives à la sécurité sans au moins un certain niveau d'assurance de sécurité impliquée dans l'identification des partenaires d'échange, et la sécurisation des canaux de communication entre eux.

Toutefois, différentes situations et applications auront différentes prescriptions en matière de sécurité, c'est pourquoi il est important que ceux qui adoptent et ceux qui mettent en œuvre considèrent bien les besoins de leurs applications spécifiques.

Par exemple, dans une application où deux partenaires d'échange ont une ligne de communication dédiée qui implémente des mesures de sécurité propres, il peut y avoir peu ou pas du tout de considérations de sécurité particulières en plus de ce que l'environnement d'échange fournit déjà.

Par ailleurs, si des informations sont communiquées sur des canaux de communication accessibles au public, il faudra vraisemblablement prendre une série de mesures de sécurité.

9.4 Capacités de politique

Toutes les applications prenant en charge la fonctionnalité de partage et d'échange d'informations de cybersécurité n'auront pas besoin d'utiliser la faculté de déclarer des restrictions, des limitations et/ou des autorisations. Toutefois, la faculté de déclarer de tels types d'information en relation avec la politique est importante dans de nombreuses situations professionnelles et personnelles.

De même qu'avec les capacités de sécurité, dans lesquelles les conditions ou situations où la fonctionnalité en relation avec la politique est fournie pour l'extérieur d'une application donnée, peut-être à cause d'accords opérationnels ou contractuels, la faculté de déclarer et de mettre en œuvre une politique au sein de l'application elle-même peut ne pas être nécessaire.

9.5 Capacités de neutralité par rapport au vendeur

La neutralité par rapport au vendeur dépend beaucoup de la situation. Si l'on est train de partager ou d'échanger des données générées par le produit d'un vendeur donnée à l'aide d'un format d'échange et/ou de protocoles d'échange spécifiques au vendeur, la neutralité par rapport au vendeur ne s'applique par réellement.

D'un autre côté, si l'objectif d'une application donnée est l'application et le support les plus larges des échanges d'information, maintenir une position neutre par rapport aux méthodes et/ou informations spécifiques au vendeur est considéré comme important.

Appendice I

Introduction au partage et à l'échange d'informations concernant la cybersécurité

(Cet appendice ne fait pas partie intégrante de la présente Recommandation)

Cet appendice décrit la structure conceptuelle d'un exemple d'application d'information concernant la cybersécurité, comme le montrent les Figures I.1 et I.2. Les deux diagrammes montrent deux vues différentes de la topologie de l'application permise par les capacités décrites dans le § 7. Bien que d'autres topologies soient possibles, la topologie indiquée inclut l'utilisation de toutes les capacités tandis que d'autres topologies et applications possibles peuvent ne nécessiter qu'un sous-ensemble des capacités décrites.

Le premier diagramme décrit le scénario où de nombreux partenaires se partagent les informations, chacun ayant des fonctionnalités, applications et informations partagées différentes. Il montre les différentes méthodes d'accès aux informations, à partir d'un nœud donné, par des applications faisant usage de ces informations.

Il faut noter que cet appendice ne proscrit pas exactement les manières et raisons pour lesquelles les informations sont utilisées, seulement qu'il est possible d'y accéder de plusieurs manières. De même, le premier diagramme montre que tous les échanges entre les nœuds sont pris en charge via l'utilisation d'un format de message normalisé.

Le deuxième diagramme est une vue en trois dimensions du premier diagramme montrant deux exemples de partenaires échangeant des informations, et décrit les capacités qu'il est probable que chacun doive implémenter pour participer lors du processus d'échange. A nouveau, comme dans le premier diagramme, les implémentations et applications réelles peuvent ne pas avoir besoin de toutes les fonctionnalités prises en charge par toutes les capacités listées et sont donc libres de choisir quelles fonctionnalités sont réellement incluses dans une implémentation/application donnée.

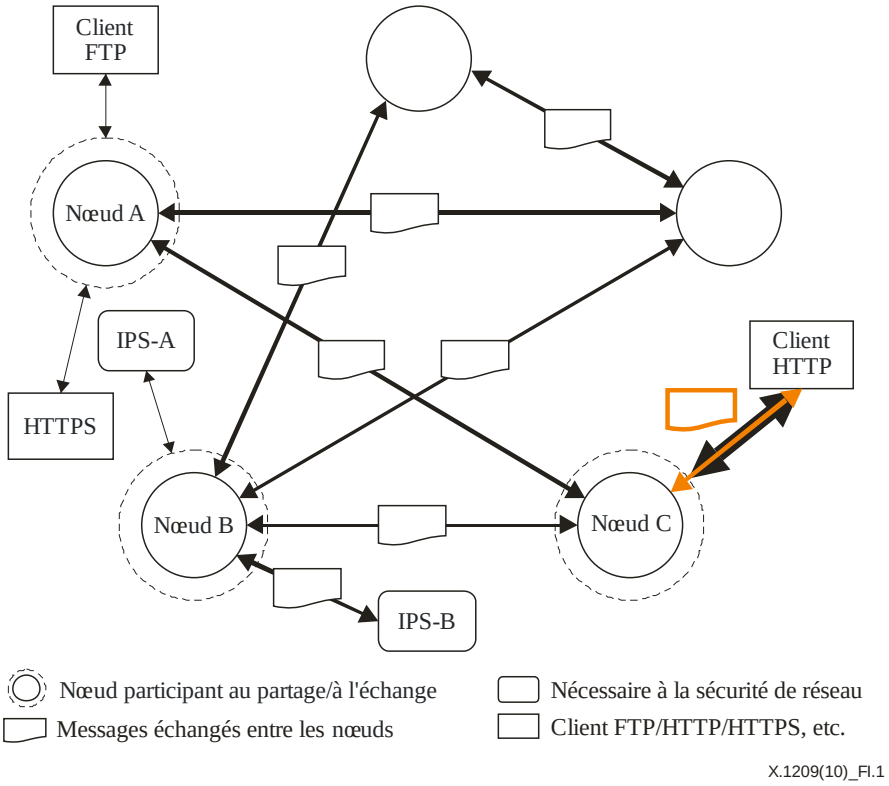

Figure I.1 – Exemple de déploiement de partage et échange d'informations concernant la cybersécurité

- Tous les nœuds participants communiquent avec chacun des autres nœuds par via des messages normalisés.

  Les capacités suivantes sont importantes dans la prise en charge de cette fonctionnalité:

  – Capacités de format/encodage (§ 8.1).

  – Capacités de transfert/échange (§ 8.2).

- Les données requises d'un nœud peuvent être en réalité fournies par un autre.

  Les capacités suivantes sont importantes dans la prise en charge de cette fonctionnalité:

  – Capacités de sécurité (§ 8.3).

  – Capacités de politique (§ 8.4).

- Un nœud donné peut implémenter des protocoles cadres uniquement, ou peut rendre disponible des données cadres par le biais d'autres protocoles/services, par exemple FTP ou HTTP sont utilisés pour accéder aux données cadres du nœud A.

  Les capacités suivantes sont importantes dans la prise en charge de cette fonctionnalité:

  – Capacités de format/encodage (§ 8.1).

  – Capacités de transfert/échange (§ 8.2).

  – Capacités de neutralité par rapport au vendeur (§ 8.5).

- Le nécessaire de sécurité, composé par exemple de deux systèmes de prévention d'intrusion IPS-A et IPS-B connectés au nœud B, peut accéder à des informations de cybersécurité, soit directement, par exemple IPS-B, soit via un service d'enveloppe, par exemple IPS-A, autorisant aux équipements d'utiliser le partage et l'échange de fonctionnalité, soit d'une manière normalisée de partage et d'échange d'informations concernant la cybersécurité, soit selon des méthodes dépendantes de l'équipement/propriétaires.

Les capacités suivantes sont importantes dans la prise en charge de cette fonctionnalité:

– Capacités de format/encodage (§ 8.1).
– Capacités de transfert/échange (§ 8.2).
– Capacités de neutralité par rapport au vendeur (§ 8.5).

- Un nécessaire de sécurité peut utiliser tout protocole ou toute couche protocolaire prenant en charge le transport de messages, par exemple TCP/IP, HTTP, HTTPS, SSL utilisés par les clients requérant les services du nœud C.

  Les capacités suivantes sont importantes dans la prise en charge de cette fonctionnalité:

  – Capacités de format/encodage (§ 8.1).
  – Capacités de transfert/échange (§ 8.2).
  – Capacités de neutralité par rapport au vendeur (§ 8.5).

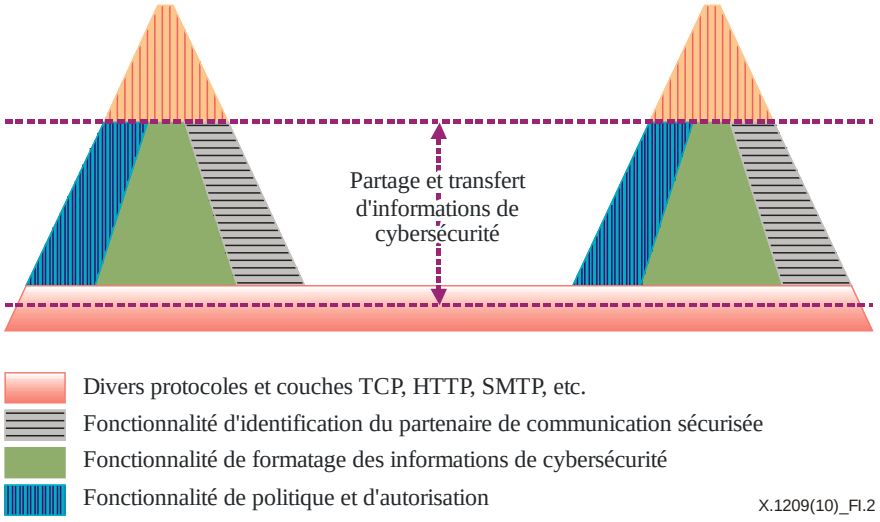

Figure I.2 – Perspective à deux nœuds

- Les nœuds participants échangent des requêtes et des réponses par le biais de divers protocoles et couches protocolaires.

  Les capacités suivantes sont importantes dans la prise en charge de cette fonctionnalité:

  – Capacités de format/encodage (§ 8.1).
  – Capacités de transfert/échange (§ 8.2).
- Pour de nombreuses applications, les méthodes fiables pour l'identification des partenaires de communication seront nécessaires.

  Les capacités suivantes sont importantes dans la prise en charge de cette fonctionnalité:

  – Capacités de sécurité (§ 8.3).
  – Capacités de politique (§ 8.4).
- Les nœuds acquièrent et utilisent les données fournies par d'autres nœuds.

  Les capacités suivantes sont importantes dans la prise en charge de cette fonctionnalité:

  – Capacités de format/encodage (§ 8.1).
  – Capacités de sécurité (§ 8.3).
  – Capacités de politique (§ 8.4).
  – Capacités de neutralité par rapport au vendeur (§ 8.5).

- Les applications utilisent différentes fonctionnalités de vérification de l'autorisation pour satisfaire les différentes prescriptions liées à la sécurité nécessaires selon l'application.

  Les capacités suivantes sont importantes dans la prise en charge de cette fonctionnalité:

  – Capacités de politique (§ 8.4).
- Les applications aux différents nœuds peuvent avoir besoin d'utiliser les informations concernant l'identité des autres nœuds pour diverses raisons, par exemple le client du nœud A requière auprès du nœud B l'accès aux informations de cybersécurité disponibles.

  Les capacités suivantes sont importantes dans la prise en charge de cette fonctionnalité:

  – Capacités de politique (§ 8.4).
- Les fonctionnalités de cœur d'un nœud participant donné sont:

  – Recevoir les informations concernant la cybersécurité.

  – Enregistrer et archiver les informations concernant la cybersécurité.

  – Faire les demandes d'informations concernant la cybersécurité.

  Les capacités suivantes sont importantes dans la prise en charge des fonctionnalités mentionnées:

  – Capacités de format/encodage (§ 8.1).

  – Capacités de transfert/échange (§ 8.2).

  – Capacités de politique (§ 8.4).
- Les applications utilisent des outils en relation, par exemple la vérification de l'authentification et de l'autorisation pour gérer les problèmes liés à l'accès.

  Les capacités suivantes sont importantes dans la prise en charge de cette fonctionnalité:

  – Capacités de sécurité (§ 8.3).

  – Capacités de politique (§ 8.4).
- Les applications utilisent un modèle de données commun pour gérer les problèmes liés à l'accès entre les nœuds.

  Les capacités suivantes sont importantes dans la prise en charge de cette fonctionnalité:

  – Capacités de format/encodage (§ 8.1).

  – Capacités de transfert/échange (§ 8.2).

  – Capacités de neutralité par rapport au vendeur (§ 8.5).
- Les applications utilisent des identifiants à la fois lors des communications entre nœuds et entre nœuds et clients.

  Les capacités suivantes sont importantes dans la prise en charge de cette fonctionnalité:

  – Capacités de sécurité (§ 8.3).

  – Capacités de politique (§ 8.4).
- Les requêtes et réponses de nœud à nœud sont considérées comme étant la "norme" alors que les applications peuvent fournir une interface de couche d'application entre requêtes et réponses de nœud à client pour les clients qui n'implémentent pas les méthodes normalisées et/ou les protocoles utilisés entre les nœuds.

  Les capacités suivantes sont importantes dans la prise en charge de cette fonctionnalité:

  – Capacités de format/encodage (§ 8.1).

  – Capacités de transfert/échange (§ 8.2).

  – Capacités de neutralité par rapport au vendeur (§ 8.5).

- Le cadre prend en charge à la fois les modes envoi et réception (*push* et *pull*) des opérations et les modes avec et sans état (*state-full* et *stateless*)

  Les capacités suivantes sont importantes dans la prise en charge de cette fonctionnalité:

  – Capacités de transfert/échange (§ 8.2).

- Les architectures des applications peuvent fournir "l'accroche" dans l'identification fiable et les modèles de données d'identification nécessaires aux applications.

  Les capacités suivantes sont importantes dans la prise en charge de cette fonctionnalité:

  – Capacités de sécurité (§ 8.3).

  – Capacités de politique (§ 8.4).

Appendice II

Activités en relation

(Cet appendice ne fait pas partie intégrante de la présente Recommandation)

II.1 Informations communes concernant la sécurité

Les informations communes concernant la sécurité sont des informations de sécurité ouvertes fournies par des organisations à but non lucratif, telles que CERT/CC, MITRE ou projet ouvert. Par exemple, il y a les informations concernant les failles et expositions communes (CVE, *common vulnerabilities and exposures*), l'énumération des faiblesses communes (CWE, *common weakness enumeration*), l'énumération des logiciels malveillants communs (CME, *common malware enumeration*) et l'énumération et la classification des schémas d'attaque communs (CAPEC, *common attack pattern enumeration and classification*), la base de données des failles au code source libre (OSVDB, *open source vulnerability database*), les signatures que fournissent [b-Snort] ou [b-Bro], et ainsi de suite.

Dans le cas de MITRE, CVE est un répertoire d'informations publiquement connues concernant les failles et expositions de sécurité. Il est utilisé comme base pour la base de données nationale des failles (NVD, *National Vulnerability Database*) développée par le *National Institute of Standards and Technology* américain. La CWE fournit un ensemble unifié, mesurable, de faiblesses logicielles permettant une discussion, une description, une sélection et une utilisation plus efficaces des outils logiciels et des services de sécurité qui peuvent trouver ces faiblesses dans le code source et les systèmes opérationnels. La CME fournit des identifiants uniques communs aux nouvelles menaces de virus et aux menaces de virus émergents les plus répandues afin de réduire la confusion du public durant les incidents liés aux logiciels malveillants. Il ne s'agit pas d'une tentative de remplacer les noms des vendeurs utilisés pour les virus et autres formes de logiciels malveillants, mais plutôt de faciliter l'adoption d'une capacité d'indexation partagée, neutre, des logiciels malveillants. La CAPEC fournit un catalogue à la disposition du public des schémas d'attaque ainsi qu'un schéma global et une taxonomie de classification.

Dans le cas d'une OSVDB, ce projet est une base de données indépendante et au code source libre créée par et pour la communauté de la sécurité. Elle sert à fournit des informations techniques précises, détaillées, actuelles et objectives sur les failles de sécurité. Elle va également promouvoir une collaboration plus grande, plus ouverte entre entreprises et particuliers, éliminant les travaux redondants et réduisant les dépenses inhérentes au développement et à la maintenance des bases de données des failles internes.

Snort est un système au code source libre de prévention et de détection des intrusions dans le réseau, utilisant un langage fondé sur des règles, qui combine les bénéfices des méthodes d'inspection basées sur la signature, le protocole et des méthodes d'inspection basées sur les anomalies. Les règles de Snort ont été rigoureusement testées contre les mêmes normes que l'équipe VRT (*Vulnerability Research Team*) utilise pour les clients.

Enfin, Bro est projet au code source libre basé sur la détection d'intrusion de réseau qui surveille passivement le trafic réseau et cherche une activité suspecte. Les règles de Bro peuvent décrire des activités, ce qui mérite que les activités le signalent, ou les signatures décrivant les attaques connues ou les accès aux failles connues.

II.2 Nouvelles informations concernant la sécurité

Les nouvelles informations concernant la sécurité sont les signatures des nouvelles menaces ou attaques, le trafic anormal, les vers inconnus, etc., automatiquement générés. La génération de signatures d'attaques fut récemment un sujet de recherche très actif, et deux solutions expérimentales, "Early bird" et "Polygraph", ont été proposées. Le rôle principal de ces solutions est

de détecter les cyberattaques et saisir les séquences d'octets, qui représentent l'identité de l'attaque. Le service de signature FirstLight ou la protection active contre les logiciels malveillants de *Endeavor Security* et ZASMIN (*Zero-day Attack Signature Management INfrastructure*) de ETRI fournissent des nouvelles signatures, qui sont constamment mises à jour, revues et étendues. Ces technologies avancées de génération de modèles qui se développent nous permettent de générer automatiquement des signatures basées sur le trafic d'attaque. Bien qu'il y ait eu une avancée dans l'amélioration de la qualité des signatures, le partage des signatures en est toujours à ses débuts.

II.3 Activités en relation pour le partage d'informations concernant la sécurité

II.3.1 Equipes de réponse aux incidents informatiques

Les équipes CIRT (CIRT, *computer incident response teams*) étudient les failles de sécurité du réseau, recherchent les modifications sur le long terme des systèmes réseaux, et développent les informations et formations pour aider à améliorer la sécurité. Elles continuent de répondre aux incidents de sécurité majeurs et analysent les failles des produits. En même temps que l'augmentation rapide de la taille de l'Internet et de son utilisation pour des fonctions critiques, il y a eu des modifications progressives dans les techniques des intrus, une augmentation des dommages, une difficulté croissante de détecter une attaque, et une difficulté croissante d'attraper les assaillants.

II.3.2 Agence européenne chargée de la sécurité des réseaux et de l'information

L'Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA, *European Network and Information Security Agency*) a présenté la première étude de faisabilité sur un système européen de partage des informations et d'alerte (EISAS, *European Information Sharing and Alert System*) pour informer les PME (petites et moyennes entreprises) et les citoyens de l'Union européenne, sur les menaces, failles et attaques. L'étude de faisabilité conclut que la façon la plus optimale pour l'UE de faciliter le partage d'informations est de se charger du rôle de facilitateur, de modérateur des discussions et de "garant des bonnes pratiques" entre systèmes nationaux de partage d'informations et d'alerte, plutôt que de prendre une fonction centrale, opérationnelle en elle-même. Afin de mener à bien l'étude, la faisabilité d'un système EISAS a dû être supposée et il a fallu la vérifier. Le système EISAS suggère un modèle général consistant en trois composantes principales et ce modèle était prévu pour identifier les zones fonctionnelles dans lesquelles un système EISAS pouvait ajouter une valeur aux activités de partage d'informations existantes au sein des Etats membres et combler les lacunes de la couverture avec les informations de sécurité des informations et du réseau (NIS, *network and information security*). Les trois composantes sont la composante de récolte des informations (IGC, *information gathering component*), la composante de traitement des informations (IPC, *information processing component*) et la composante de dissémination des informations (IDC, *information dissemination component*).

II.3.3 Forum des réponses aux incidents et des équipes de sécurité

Le forum des réponses aux incidents et des équipes de sécurité (FIRST, *Forum of Incident Response and Security Teams*) est la première organisation et un chef de file reconnu internationalement dans la réponse aux incidents. L'appartenance au forum FIRST permet aux équipes de réponse aux incidents de répondre plus efficacement aux incidents de sécurité – de manière réactive aussi bien que proactive. Ce forum rassemble une variété d'équipes de réponse aux incidents de sécurité informatiques provenant d'organisations gouvernementales, commerciales et à caractère éducatif. L'objectif de ce forum est d'encourager la coopération et la coordination dans la prévention des incidents, pour stimuler une réaction rapide aux incidents et de promouvoir le partage d'informations entre membres et avec la communauté au sens large.

II.3.4 Equipe de réponse d'urgence informatique de l'Asie Pacifique

L'équipe de réponse d'urgence informatique de l'Asie Pacifique APCERT (APCERT, *Computer Emergency Response Team*) coopère avec les équipes de réponse d'urgence informatique CERT (CERT, *Computer Emergency Response Team*) et les équipes de réponse aux incidents de sécurité informatique CSIRT (CSIRT, *Computer Security Incidence Response Team*) pour assurer la sécurité de l'Internet dans la région d'Asie Pacifique, basée sur un véritable partage d'informations, la confiance et la coopération. Elles facilitent le partage d'informations et l'échange de technologies, y compris les informations de sécurité, les virus et le code malveillant, entre ses membres. Elles promeuvent également la recherche et le développement collaboratifs sur des sujets d'intérêt pour ses membres, et fournissent des recommandations afin d'aider à aborder les questions juridiques en relation avec les informations concernant la sécurité et les réponses d'urgence au-delà des frontières régionales.

II.3.5 Centre de partage et d'analyse des informations pour les télécommunications

L'Internet et les autres réseaux de télécommunication forment la base d'une structure sociale et économique à l'échelle mondiale. Assurer la sécurité de l'information devient un problème urgent dans la vie sociale et économique. Le Centre de partage et d'analyse des informations pour les télécommunications (Telecom-ISAC, *Information Sharing and Analysis Center*) a pour objectif de rassembler, analyser et partager les informations concernant les incidents et prend les mesures opportunes pour assurer des opérations sans problèmes et stables des services de télécommunication. En outre, le centre ISAC crée un forum avec une grande variété de membres collaborant pour partage leurs points de vue et expériences, y compris sur les informations concernant les risques, les failles et les solutions en matière de sécurité, et ainsi de suite.

Appendice III

Activités en relation

(Cet appendice ne fait pas partie intégrante de la présente Recommandation)

[APCERT]	Asia Pacific Computer Emergency Response Team. http://www.apcert.org
[CERT]	Computer Emergency Response Team. http://www.cert.org
[ENDEAVOR]	Endeavor Security. http://www.endeavorsecurity.com
[FIRST]	Forum of Incident Response and Security Team. http://www.first.org
[MITRE]	MITRE. http://makingsecuritymeasurable.mitre.org/
[Telecom-ISAC]	Telecom information sharing and Analysis Center. https://www.telecom-isac.jp
[WIKI]	Wikipedia. http://en.wikipedia.org

Bibliographie

[b-ITU-T X.1205] Recommandation UIT-T X.1205 (2008), *Présentation générale de la cybersécurité*.

[b-Bro] Bro (novembre 2004), *Quick Start Guide Manual*.

[b-EISAS] European information sharing and Alert System (2006/2007), *A feasibility study*.

[b-OSVDB] Open Source Vulnerability DataBase. *Project Aims and Objectives*.

[b-Snort] Snort (mai 2008). *Snort User Manual 2.8.2*.

[b-ZASMIN] Information Security Research Division of ETRI, *Zero-day Attack Signature Management Infrastructure*.

SÉRIES DES RECOMMANDATIONS UIT-T

Série A	Organisation du travail de l'UIT-T
Série D	Principes généraux de tarification
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	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	Terminaux et méthodes d'évaluation subjectives et objectives
Série Q	Commutation et signalisation
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 et réseaux de prochaine génération
Série Z	Langages et aspects généraux logiciels des systèmes de télécommunication

Imprimé en Suisse
Genève, 2011