Manuel sur la sécurité de L'UIT-T – 4e édition

- Spécifications et architectures de sécurité
- Aspects de gestion de la sécurité
- L'annuaire, authentification et gestion d'identité
- Sécurisation de l'infrastructure des réseaux
- Approches particulières relatives à la sécurité des réseaux
- Sécurité des applications
- Lutte contre les menaces courantes dans les réseaux
- L'avenir de la normalisation de la sécurité dans les TIC/ télécommunications

Feuille de route sur les normes de sécurité dans les TIC

Partie 1: Organisations s'occupant de normalisation des TIC et leurs activités

Partie 2: Normes approuvées relatives à la sécurité des TIC (qui contient une base de données avec des liens directs)

Partie 3: Normes de sécurité en cours d'élaboration

Partie 4: Besoins futurs et propositions de nouvelles normes de sécurité

Partie 5: Bonnes pratiques en matière de sécurité

Partie 6: La situation en matière de gestion d'identité (IdM)

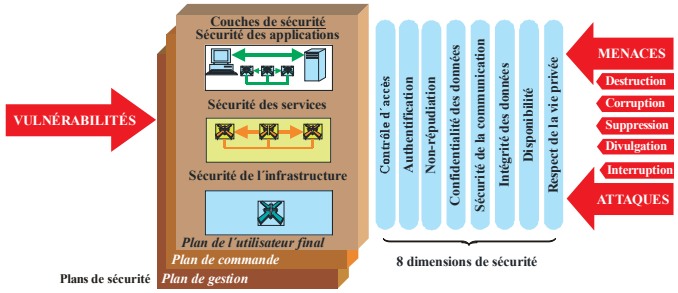
Recueil sur la sécurité

- Catalogue des Recommandations approuvées relatives à la sécurité des télécommunications
- Liste des définitions relatives à la sécurité extraites des Recommandations UIT-T approuvées
- Présentation succincte des Commissions d'études de l'UIT-T menant des acticités dans le domaine de la sécurité
- Présentation succincte des Recommandations faisant l'objet d'un examen relatif aux considérations de sécurité
- Présentation succincte des autres activités de l'UIT dans le domaine de la sécurité.

Architectures de sécurité

La Rec. UIT-T X.805 sur "l'architecture de sécurité pour les systèmes assurant des communications de bout en bout", ainsi qu'un certain nombre d'architectures propres à certaines applications, ont été mises au point pour couvrir divers domaines, par exemple la gestion de réseau, les communications entre homologues et les serveurs web mobiles.

L'architecture X.805, illustrée plus haut, est définie sur la base de trois principaux concepts pour les réseaux de bout en bout: les couches, les plans et les dimensions de sécurité. On adopte une approche hiérarchique de subdivision des spécifications de sécurité entre les couches et les plans de manière à assurer la sécurité de bout.



Cette architecture peut servir de base à une évaluation de la sécurité ou servir de guide pour élaborer des politiques de sécurité, des plans d'intervention en cas d'incident et de retour à la normale, et des architectures techniques compte tenu des dimensions de sécurité applicables dans chaque couche et chaque plan de sécurité dans la phase de définition et de planification.

www.itu.int/itu-t/studygroups

Sécurité

Etablir la confiance et la sécurité dans l'utilisation des TIC

(SMSI – Grande orientation C.5)

01.2012 tsbpromo@itu.int

UIT-T

La sécurité dans les télécommunications/TIC

L'UIT-T travaille dans le domaine de la sécurité des télécommunications/TIC depuis plus de vingt ans. Plusieurs Commissions d'études ont élaboré des Recommandations et des orientations dans un certain nombre de domaines essentiels. Les travaux de l'UIT-T sur la sécurité sont maintenant essentiellement confiés à la Commission d'études 17, qui a été désignée Commission d'études directrice pour la sécurité.

Protection des actifs

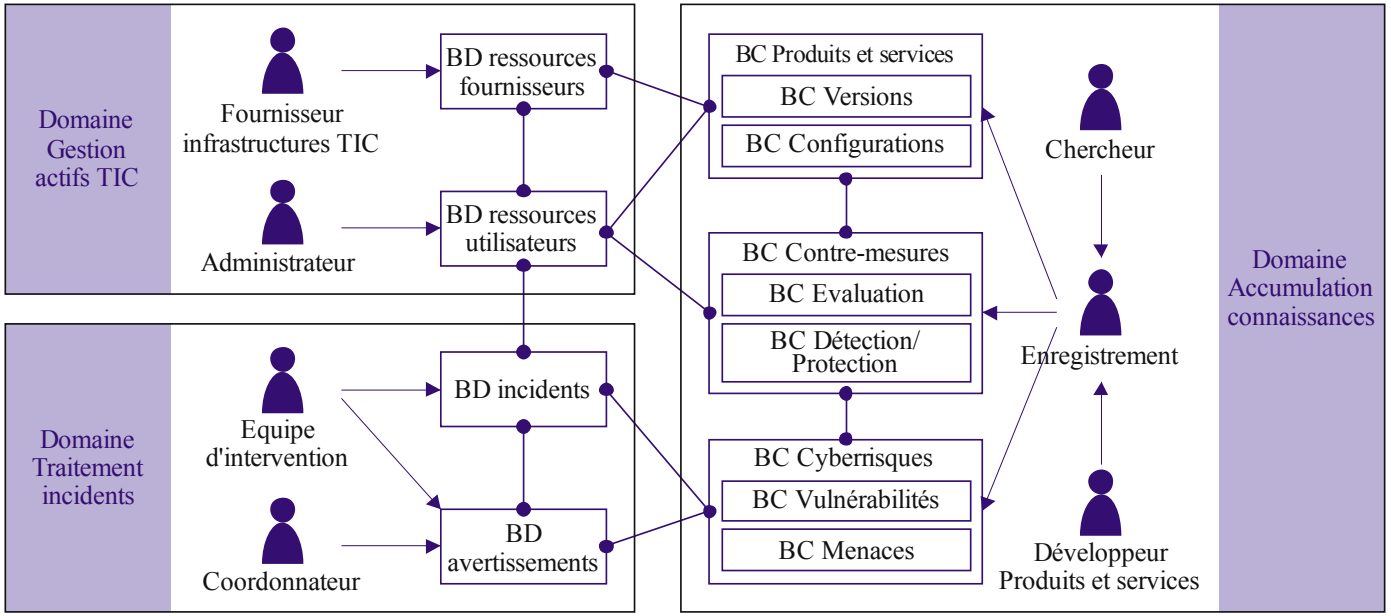
D'une manière générale, dans le domaine de la sécurité des TIC, les parties pouvant nécessiter une protection des actifs sont les suivantes:

- Les clients/abonnés, qui veulent que le réseau et les services offerts soient fiables et que les services soient disponibles (notamment les services d'urgence).
- La communauté/les autorités publiques, qui exigent que la sécurité fasse l'objet de directives et/ou de lois, afin de garantir la disponibilité des services, une concurrence loyale et la protection de la vie privée.
- Les opérateurs de réseau/fournisseurs de service proprement dits, qui ont besoin de sécurité pour sauvegarder leurs intérêts opérationnels et commerciaux et pour satisfaire à leurs obligations vis-à-vis des clients et du grand public, au niveau national comme au niveau international.

Rec. UIT-T série X.1500 – Modèle général d'échange d'informations sur la cybersécurité

Les techniques d'échange d'information (CYBEX) sont composées de fonctions de base pouvant être utilisées séparément ou ensemble, selon qu'il conviendra. Ces fonctions sont les suivantes:

- Structuration des informations sur la cybersécurité à des fins d'échange.
- Identification et découverte d'informations sur la cybersécurité et d'entités.
- Etablissement d'accords de confiance et de politiques d'échange d'informations entre entités échangeant de telles informations.
- Demandes et réponses concernant les informations sur la cybersécurité.
- Assurer l'intégrité des échanges d'informations sur la cybersécurité.



BD = base de données, BC = base de connaissances

Ce schéma illustre l'ontologie de CYBEX, présentée sous la forme d'un contrat d'opérations. Les opérations de cybersécurité se divisent pour l'essentiel en trois domaines: traitement des incidents, gestion des actifs TIC et accumulation de connaissances.