Union internationale des télécommunications

UIT-T

SECTEUR DE LA NORMALISATION
DES TÉLÉCOMMUNICATIONS
DE L'UIT

X.1205

(04/2008)

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

Sécurité du cyberespace – Cybersécurité

Présentation générale de la cybersécurité

Recommandation UIT-T X.1205

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

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

Recommandation UIT-T X.1205

Présentation générale de la cybersécurité

Résumé

La Recommandation UIT-T X.1205 contient une définition de la cybersécurité. Elle décrit les différentes menaces contre la sécurité du point de vue d'une organisation et présente les menaces et vulnérabilités relatives à la cybersécurité ainsi que les outils habituellement utilisés par les pirates. Les menaces sont examinées dans diverses couches de réseau.

Ce document expose diverses technologies de cybersécurité disponibles pour remédier aux menaces: routeurs, pare-feu, protection antivirus, systèmes de détection des intrusions, systèmes de protection contre les intrusions, informatique sécurisée, audit et surveillance, etc. Il aborde les principes de protection des réseaux, par exemple la défense en profondeur et la gestion d'accès appliquée à la cybersécurité. Il traite des stratégies et techniques de gestion des risques, y compris de l'importance de la formation et de la sensibilisation à la protection du réseau. Enfin, des exemples sont fournis concernant la sécurisation de divers réseaux compte tenu des technologies présentées.

Source

La Recommandation UIT-T X.1205 a été approuvée le 18 avril 2008 par la Commission d'études 17 (2005-2008) de l'UIT-T selon la procédure définie dans la Résolution 1 de l'AMNT.

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.1205

Présentation générale de la cybersécurité

1 Domaine d'application

La présente Recommandation contient une définition de la cybersécurité au § 3. Elle décrit les différentes menaces contre la sécurité du point de vue d'une organisation.

NOTE – L'utilisation du terme "identité" dans la présente Recommandation ne lui confère pas une valeur absolue, et ne constitue pas en particulier une validation positive.

Le § 7 traite de la nature de l'environnement de cybersécurité dans les entreprises, des risques liés à la cybersécurité et de la sécurité des communications de bout en bout. Le § 8 aborde les stratégies possibles de protection des réseaux, notamment la gestion de politique en boucle fermée et la gestion d'accès uniforme. Il porte aussi sur les techniques de sécurisation des communications, la sécurité à profondeur variable, la sécurisation du plan de gestion, la sécurité par couches et la capacité de survie du réseau même après une attaque.

L'Appendice I décrit les différentes menaces contre la sécurité et présente les outils habituellement utilisés par les pirates.

L'Appendice II passe en revue la palette des technologies de cybersécurité: cryptographie, techniques de contrôle d'accès, techniques de protection périmétrique, antivirus et intégrité du système, audit et surveillance, et gestion.

L'Appendice III donne des exemples de sécurité dans les réseaux. Il présente notamment des exemples de sécurisation de l'accès à distance, de la téléphonie IP, des clients VoIP, des bureaux distants et des réseaux WLAN.

2 Références

Les Recommandations UIT-T et autres références suivantes contiennent des dispositions qui, par suite de la référence qui y est faite, constituent des dispositions de la présente Recommandation. Au moment de la publication, les éditions indiquées étaient en vigueur. Les Recommandations et autres références étant sujettes à révision, les utilisateurs de la présente Recommandation sont invités à rechercher la possibilité d'appliquer les éditions les plus récentes des Recommandations et autres références énumérées ci-dessous. Une liste des Recommandations UIT-T en vigueur est publiée périodiquement. La référence à un document figurant dans la présente Recommandation ne donne pas à ce document en tant que tel le statut de Recommandation.

[UIT-T X.800] Recommandation UIT-T X.800 (1991), *Architecture de sécurité pour l'interconnexion en systèmes ouverts d'applications du CCITT*.

[UIT-T X.805] Recommandation UIT-T X.805 (2003), *Architecture de sécurité pour les systèmes assurant des communications de bout en bout*.

[UIT-T X.811] Recommandation UIT-T X.811 (1995) | ISO/CEI 10181-2:1996, *Technologies de l'information – Interconnexion des systèmes ouverts – Cadres de sécurité pour les systèmes ouverts: cadre d'authentification*.

[UIT-T X.812] Recommandation UIT-T X.812 (1995) | ISO/CEI 10181-3:1996, *Technologies de l'information – Interconnexion des systèmes ouverts – Cadres de sécurité pour les systèmes ouverts: cadre de contrôle d'accès*.

[IETF RFC 1918] IETF RFC 1918 (1996), *Address Allocation for Private Internets* <http://www.ietf.org/rfc/rfc1918.txt?number=1918>.

[IETF RFC 2396] IETF RFC 2396 (1998), *Uniform Resource Identifiers (URI): Generic Syntax* <http://www.ietf.org/rfc/rfc2396.txt?number=2396>.

3 Définitions

3.1 Termes définis ailleurs

La présente Recommandation utilise les termes suivants définis ailleurs:

3.1.1 La présente Recommandation utilise les termes suivants définis dans le document [UIT-T X.800]:

a) autorisation;

b) architecture de sécurité;

c) politique de sécurité;

d) utilisateur.

3.1.2 La présente Recommandation utilise les termes suivants définis dans le document [UIT-T X.805]:

a) dimension de sécurité;

b) service de sécurité.

3.1.3 La présente Recommandation utilise les termes suivants définis dans le document [UIT-T X.811]:

a) authentification;

b) principe.

3.1.4 La présente Recommandation utilise les termes suivants définis dans le document [UIT-T X.812]:

a) informations de contrôle d'accès;

b) accès;

c) contrôle d'accès;

d) utilisateur.

3.1.5 La présente Recommandation utilise les termes suivants définis dans le document [IETF RFC 2396]:

a) identificateur universel de ressource (URI).

b) référence d'URI.

3.2 Termes définis dans la présente Recommandation

Les termes suivants sont définis dans la présente Recommandation:

3.2.1 **point d'accès**: pivot sans fil IEEE 802.11, type particulier de station (STA) fonctionnant comme un point d'accès.

3.2.2 **ensemble de services de base (BSS, *basic service set*)**: zone de couverture desservie par un seul point d'accès (AP, *access point*).

3.2.3 **algorithme cryptographique**: procédé de chiffrement permettant de modifier les données pour les camoufler.

3.2.4 **cyberenvironnement**: ensemble des utilisateurs, réseaux, dispositifs, logiciels, processus, informations en mémoire ou en cours de transmission, applications, services et systèmes qui peuvent être raccordés directement ou indirectement à des réseaux.

3.2.5 cybersécurité: 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.

3.2.6 système réparti: support non normalisé pour l'interconnexion d'ensembles BSS dans un ensemble ESS.

3.2.7 protocole d'authentification extensible: extension PPP prenant en charge des méthodes d'authentification supplémentaires, définie dans la spécification [b-IEEE 802.1X].

3.2.8 ensemble de services étendus (ESS*, extended service set*): réseau local sans fil unique avec des ensembles BSS dans un seul sous-réseau IP.

3.2.9 pare-feu: système ou combinaison de systèmes établissant une frontière entre deux réseaux ou plus. Il s'agit d'une passerelle qui limite l'accès entre réseaux conformément à une politique de sécurité locale.

3.2.10 agent étranger: routeur du réseau visité/hôte qui dessert le nœud mobile lorsque celui-ci est en visite dans le réseau hôte. L'agent étranger gère la tunnellisation et l'acheminement entre le nœud mobile et les autres nœuds ainsi qu'entre le réseau de rattachement du mobile et le réseau hôte.

3.2.11 pot de miel, leurre informatique: programme logiciel qui émule un réseau afin d'attirer (et éventuellement de démasquer) les intrus et de suivre leurs actions. Les résultats obtenus par ce type de systèmes peuvent servir à déterminer les intentions de l'intrus et à rassembler des preuves.

3.2.12 agent résidentiel: routeur qui dessert le nœud mobile lorsque celui-ci est en visite dans d'autres réseaux. L'agent résidentiel tient à jour les informations sur l'emplacement actuel de ce nœud mobile.

3.2.13 point d'accès public: endroit public où les utilisateurs IEEE 802.11 mobiles peuvent se raccorder à l'Internet.

3.2.14 mobilité IP: mécanisme offrant une connectivité plus transparente aux nœuds mobiles qui "visitent" différents sous-réseaux IP au cours de leur déplacement. Il s'agit d'un mécanisme de gestion des nœuds mobiles à la fois dans les réseaux filaires et dans les réseaux sans fil.

4 Abréviations

La présente Recommandation utilise les abréviations suivantes:

3DES norme de chiffrement de données triple (*triple data encryption standard*)

AAA authentification, autorisation et comptabilité (*authentication, authorization and accounting*)

ACL liste de contrôle d'accès (*access control list*)

AES norme de chiffrement perfectionné (*advanced encryption standard*)

AP point d'accès (*access point*)

ASP fournisseur de services d'application (*application service provider*)

BSS ensemble de services de base (*basic service set*)

CA autorité de certification (*certification authority*)

CMP protocole de gestion des certificats (*certificate management protocol*)

COPS service commun de politique ouverte (*common open policy service*)

CRL liste de révocation de certificats (*certificate revocation list*)

DISA accès direct au système (*direct inward system access*)

DNS système de noms de domaine (*domain name system*)

EAP protocole d'authentification extensible (*extensible authentication protocol*)

EMS système de gestion d'élément (*element management system*)

ESS ensemble de services étendus (*extended service set*)

ESSID identificateur d'ensemble de services étendus (*extended service set identifier*)

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

HMAC code MAC fondé sur une fonction de hachage (*hash function based MAC*)

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

IDS système de détection des intrusions (*intrusion detection system*)

IKE échange de clés Internet (*Internet key exchange*)

IP protocole Internet (*Internet protocol*)

IPSec sécurité du protocole Internet (*Internet protocol security*)

ISP fournisseur de services Internet (*Internet service provider*)

L2TP protocole de tunnellisation de couche 2 (*layer 2 tunnelling protocol*)

LAN réseau local (*local area network*)

MAC code d'authentification de message (*message authentication code*)

MD5 algorithme 5 de condensé de message (*message digest algorithm 5*)

MIC contrôle d'intégrité de message (*message integrity check*)

MIME extensions de messagerie Internet à fonctions multiples (*multipurpose Internet mail extensions*)

MPLS commutation par étiquette multiprotocole (*multiprotocol label switching*)

MU unité mobile (*mobile unit*)

NAT traduction d'adresse réseau (*network address translation*)

NGN réseau de prochaine génération (*next generation network*)

NIC carte d'interface réseau (*network interface card*)

NOC centre d'exploitation du réseau (*network operations center*)

OAM&P exploitation, administration, maintenance et approvisionnement (*operations, administration, maintenance & provisioning*)

OCSP protocole d'état de certificat en ligne (*online certificate status protocol*)

OS	système d'exploitation (*operating system*)
OSI	interconnexion des systèmes ouverts (*open systems interconnection*)
PDP	point de décision de politique (*policy decision point*)
PEAP	protocole EAP protégé (*protected EAP protocol*)
PEP	point d'application de politique (*policy enforcement point*)
PGP	confidentialité plutôt bonne (*pretty good privacy*)
PKI	infrastructure de clé publique (*public key infrastructure*)
PKIX	infrastructure de clé publique X.509 (*public key infrastructure X.509*)
PoP	preuve de possession (*proof of possession*)
PPP	protocole point à point (*point-to-point protocol*)
RTPC	réseau téléphonique public commuté
RADIUS	service d'authentification à distance des utilisateurs entrants (*remote authentication dial-in user service*)
RSA	algorithme à clé publique de Rivest, Shamir et Adleman (*Rivest Shamir Adleman public key algorithm*)
SHA-1	algorithme 1 de hachage sécurisé (*secure hash algorithm 1*)
SIP	protocole d'ouverture de session (*session initiation protocol*)
SMTP	protocole simple de transfert de courrier (*simple mail transfer protocol*)
SNMP	protocole simple de gestion de réseau (*simple network management protocol*)
SP	fournisseur de services (*service provider*)
SSH	connecteur sécurisé (*secure shell*)
SSID	identification d'ensemble de services (*service set identification*)
SSO	identification unique (*single sign on*)
TKIP	protocole d'intégrité de clé temporelle (*temporal key integrity protocol*)
TLS	protocole de sécurité dans la couche transport (*transport layer security protocol*)
UE	équipement d'utilisateur (*user equipment*)
URI	identificateur universel de ressource (*uniform resource identifier*)
UTC	temps universel coordonné (*coordinated universal time*)
VAR	revendeur de services à valeur ajoutée (*value-added reseller*)
VLAN	réseau local virtuel (*virtual LAN*)
VoIP	voix sur IP, téléphonie IP (*voice over IP*)
VPLS	service de réseau local privé virtuel (*virtual private LAN service*)
VPN	réseau privé virtuel (*virtual private network*)
VPWS	service de liaison privée virtuelle (*virtual private wire service*)
WAN	réseau étendu (*wide area network*)
WEP	confidentialité équivalente à celle d'un réseau filaire (*wired equivalent privacy*)
WLAN	réseau local sans fil (*wireless LAN*)

WPA accès protégé Wi-Fi (*Wi-Fi protected access*)

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

5 Conventions

Dans la présente Recommandation, un équipement d'utilisateur (UE) désigne au sens large toutes sortes de dispositifs, entités (matérielles ou logicielles), mobiles et/ou fixes, ordinateurs personnels (PC), terminaux (multimédias), téléphones, etc., tous situés dans les locaux de l'utilisateur et souvent hors de contrôle d'un opérateur ou fournisseur de services.

6 Introduction

L'utilisation de réseaux pour raccorder des systèmes informatiques hétérogènes permet d'améliorer la productivité des organisations et d'offrir de nouvelles capacités grâce aux systèmes mis en réseau. De nos jours, il est relativement facile d'obtenir des informations, de communiquer ainsi que de surveiller et de commander des systèmes informatiques couvrant de grandes distances. En tant que tels, les réseaux actuels jouent un rôle fondamental dans les infrastructures essentielles de nombreux pays, à savoir le commerce électronique, les communications vocales et de données, les services publics, les services financiers, la santé, les transports et la défense.

La connectivité des réseaux et l'accès ubiquitaire sont des aspects essentiels des systèmes informatiques actuels. Toutefois, l'accès élargi et le faible couplage des systèmes informatiques interconnectés peuvent être des facteurs déterminants de vulnérabilité étendue. Les menaces visant les systèmes en réseau comme les attaques par déni de service, le vol de données financières et personnelles, les défaillances de réseau et l'interruption de communications vocales et de données sont en augmentation.

Les protocoles de réseau actuellement utilisés ont été mis en œuvre dans un environnement de confiance. Les nouveaux investissements et développements sont surtout consacrés à l'élaboration de nouvelles fonctionnalités et non à la sécurisation de ces fonctionnalités.

Les menaces contre la cybersécurité croissent rapidement. Les virus, vers, chevaux de Troie, attaques par usurpation d'identité, "vols d'identité"[1], spams et cyberattaques sont en augmentation. Il est nécessaire de comprendre la cybersécurité afin d'élaborer une base de connaissances qui puisse faciliter la sécurisation des réseaux de demain.

Les entreprises privées et les organismes publics sont encouragés à considérer la sécurité comme un axe de réflexion sur la façon de protéger les systèmes, les réseaux, les applications et les ressources, l'idée de départ étant que des réseaux connectés présentent des risques intrinsèques. Toutefois, la sécurité ne devrait pas représenter un obstacle pour les activités. L'objectif est de déterminer comment offrir les services nécessaires de façon sécurisée.

Dans l'environnement actuel des entreprises, le concept de périmètre disparaît. Les frontières entre réseau interne et réseau externe sont de plus en plus minces. Les applications fonctionnent sur les réseaux sur la base de couches. La sécurité est supposée exister entre chacune de ces couches. Une approche de la sécurité par couches permet aux organisations de créer plusieurs niveaux de défense contre les menaces.

---

[1] Le terme "vol d'identité" désigne uniquement l'utilisation non autorisée des identificateurs et autres informations qui, ensemble, caractérisent l'identité d'un utilisateur donné. Contrairement au concept habituel du vol, pour lequel la victime est dépossédée physiquement d'une chose, le vol d'identité consiste généralement à intercepter ou à copier des données d'identité sans que le propriétaire légitime ne s'en rende compte.

7 Cybersécurité

Les organisations doivent mettre au point un plan détaillé pour répondre à leurs besoins de sécurité. Elles sont encouragées à considérer la sécurité comme un axe de réflexion sur la façon de protéger les systèmes, les réseaux, les applications et les ressources.

7.1 Qu'est-ce que la cybersécurité?

Dans la présente Recommandation, le terme cybersécurité est défini au § 3.2.5.

Des techniques de cybersécurité peuvent être utilisées pour garantir la disponibilité des systèmes, l'intégrité, l'authenticité, la confidentialité et la non-répudiation, pour garantir le respect de la vie privée des utilisateurs ainsi que pour établir la fiabilité des utilisateurs.

Des technologies telles que les réseaux sans fil et la téléphonie IP (VoIP) permettent d'accroître l'étendue de l'Internet. A cet égard, le cyberenvironnement comporte les utilisateurs, l'Internet, les dispositifs informatiques qui lui sont raccordés et l'ensemble des applications, services et systèmes qui peuvent être raccordés directement ou indirectement à l'Internet et à l'environnement des réseaux de prochaine génération (NGN), ces derniers étant publics ou privés. Ainsi, avec la technologie VoIP, un téléphone de bureau fait partie du cyberenvironnement. Quant aux dispositifs isolés, ils peuvent eux aussi faire partie du cyberenvironnement s'ils peuvent partager des informations avec des dispositifs informatiques connectés, par le biais de supports amovibles.

Le cyberenvironnement inclut les logiciels utilisés dans les dispositifs informatiques, les informations stockées (et les informations transmises) sur ces dispositifs et les informations qui sont produites par ces dispositifs. Les installations et bâtiments qui hébergent ces dispositifs font également partie du cyberenvironnement. Il faut prendre en considération ces éléments dans le cadre de la cybersécurité.

La cybersécurité a pour objet de sécuriser le cyberenvironnement, qui est un système auquel participent des intéressés relevant de nombreuses organisations publiques ou privées, en utilisant divers composants et diverses approches en matière de sécurité. Cela étant, il est utile de concevoir la cybersécurité comme suit:

– Ensemble des politiques et des actions qui sont utilisées pour protéger les réseaux connectés (y compris les ordinateurs, dispositifs, matériels, informations stockées et informations en transit) contre l'accès non autorisé, les modifications, le vol, les perturbations, l'interruption et d'autres menaces.
– Evaluation et surveillance permanentes des politiques et actions susmentionnées afin que la qualité de service continue d'être garantie face à l'évolution de la nature des menaces.

Les spécifications des réseaux NGN énoncées dans le document [b-UIT-T Y.2201] peuvent être utilisées pour renforcer la cybersécurité de ces réseaux. Il est notamment recommandé de prendre en charge l'authentification et d'envisager la possibilité d'authentifier séparément les dispositifs et les utilisateurs. Dans les NGN, une authentification bilatérale multifactorielle avec autorisation au niveau de chaque service réduit les risques d'attaques ciblées sur les utilisateurs.

7.2 Nature de l'environnement de cybersécurité dans les entreprises

Les organisations doivent mettre au point un plan détaillé pour répondre à leurs besoins de sécurité. La sécurité n'est pas "à taille unique" (cf. [UIT-T X.805]). Elle ne peut pas être assurée par un ensemble de modules interconnectés ensemble. Les organisations sont encouragées à considérer la sécurité comme un axe de réflexion sur la façon de protéger les systèmes, les réseaux, les applications et les services de réseau.

La sécurité doit englober toutes les couches de réseau. L'adoption d'une approche de la sécurité par couches conjuguée à une gestion et à une application de politique efficaces permet d'offrir aux

professionnels de la sécurité un ensemble de solutions de sécurité qui peuvent être modulaires, souples et évolutives.

La sécurité est difficile à tester, à prévoir et à mettre en œuvre. Elle n'est pas "à taille unique". Les besoins de sécurité et la stratégie de sécurité recommandée varient suivant les organisations. Par exemple, l'ensemble des impératifs commerciaux varie suivant l'entreprise, le fournisseur de télécommunications, l'opérateur de réseau ou le fournisseur de services, qui peut faire évoluer son environnement de réseau en fonction de ces impératifs.

Une "entreprise fermée", par exemple, utilise des lignes privées logiques (relais de trame, etc.) ou physiques entre les sites, un accès à distance étant fourni de façon sélective aux employés qui ont besoin d'un accès à l'Internet. La présence sur le web est assurée par le biais d'un centre de données Internet géré par un fournisseur de services (qui est chargé d'établir un environnement sécurisé). L'organisation offre par ailleurs un accès commuté classique aux employés travaillant à distance (par exemple depuis un hôtel). Elle utilise un système de messagerie électronique privé entre les employés sans accès externe. Des réseaux locaux sans fil sont également employés.

Une "entreprise étendue" – fournisseur de télécommunications, opérateur de réseau ou fournisseur de services – peut, suivant son modèle de fonctionnement, offrir à ses employés à distance et à ses bureaux distants un accès sur VPN IP sur l'Internet, ou un débit plus élevé et une connectivité moins onéreuse y compris un accès global à l'Internet, par exemple un interfonctionnement entre les systèmes de messagerie électronique internes et le reste du monde.

Dans une "entreprise ouverte", le modèle de fonctionnement peut s'appuyer sur l'Internet pour permettre aux partenaires, fournisseurs et clients d'accéder à un centre de données Internet géré par l'entreprise, voire pour leur offrir un accès sélectif à des bases de données et applications internes (par exemple dans le cadre d'un système de gestion de la chaîne logistique). Les utilisateurs internes et les utilisateurs externes accèdent au réseau de l'entreprise depuis leur domicile, des bureaux distants ou d'autres réseaux, en utilisant des dispositifs filaires ou mobiles. A cet égard, une entreprise ouverte a des besoins de sécurité différents de ceux des autres types d'entreprise.

La Figure 7-1 présente de façon succincte ces types d'entreprise.

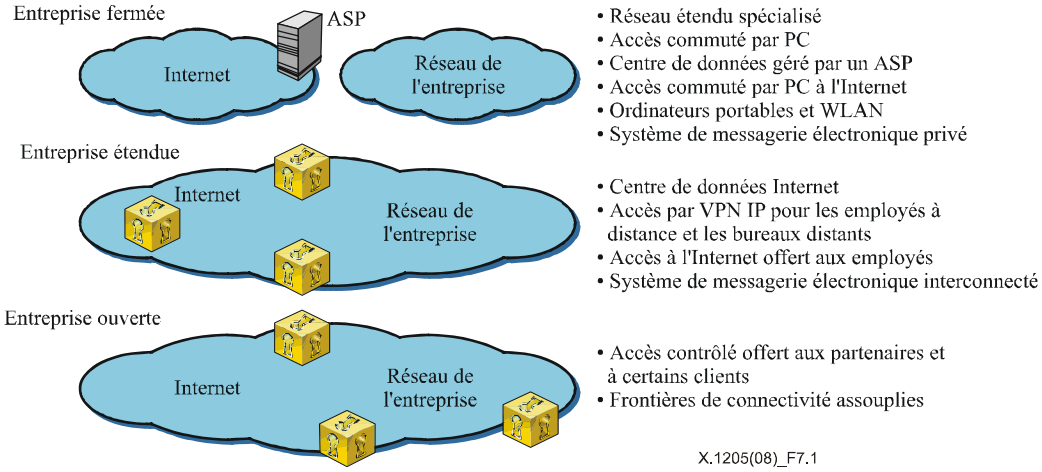

Figure 7-1 – Types génériques d'entreprise

La cybersécurité nécessite une gestion des risques. Pour cela, il faut identifier l'ensemble des composants qui doivent être protégés. Pour faciliter l'analyse des risques, il est utile de considérer que les attaques appartiennent aux catégories suivantes:

1) Attaques entraînant une interruption de service: les attaques de ce type désactivent l'accès des utilisateurs aux services voulus de façon temporaire ou permanente. Des utilisateurs

peuvent par exemple être privés de l'accès à un site web ou se trouver dans l'impossibilité de réaliser une transaction financière ou de lancer un appel vocal. Plusieurs types d'attaques peuvent conduire à une interruption de service. Par exemple, des attaques par déni de service (DoS) ou par déni de service réparti (DDoS) ou un endommagement de bâtiments qui hébergent des infrastructures essentielles peuvent avoir pour résultat la privation de l'accès à un service par les utilisateurs.

2) Atteintes aux actifs: les attaques de ce type font intervenir le vol ou une utilisation abusive d'une partie de l'infrastructure. Elles peuvent avoir une incidence sur la cybersécurité si elles sont commises à une grande échelle.

3) Détournement de composants: dans les attaques de ce type, les attaquants prennent le contrôle de certains dispositifs puis les utilisent pour lancer de nouvelles attaques contre d'autres composants du cyberenvironnement.

Un élément donné du cyberenvironnement peut être envisagé sous l'angle des risques de sécurité, qui sont généralement déterminés sur la base d'une évaluation des menaces. L'analyse des menaces passe par la description des types d'attaques possibles, des attaquants potentiels et de leurs méthodes d'attaque ainsi que des conséquences des attaques qui réussissent. Par ailleurs, dans la présente Recommandation, une vulnérabilité désigne une faiblesse susceptible d'être exploitée par un attaquant. Une évaluation des risques combinée à une analyse des menaces permet à une organisation d'évaluer les risques potentiels auxquels est exposé son réseau.

Les attaques peuvent provenir du cyberenvironnement, par le biais de vers ou d'autres maliciels, par une attaque directe visant les infrastructures essentielles (câbles de télécommunication par exemple) ou par les actions d'un utilisateur interne de confiance. Une combinaison de ces attaques est également possible. Les risques sont souvent classés comme étant élevés, moyens ou faibles. Le niveau de risque varie suivant les composants du cyberenvironnement.

Qui dit sécurité dit gestion des risques. Pour gérer les risques, de nombreuses techniques peuvent être employées. On peut par exemple élaborer une stratégie de défense qui spécifie les mesures à prendre pour contrer les éventuelles attaques. La détection permet d'identifier une attaque en cours ou passée. La formulation d'une réponse à une attaque permet de spécifier l'ensemble des mesures à prendre pour arrêter l'attaque ou pour en réduire l'incidence. La formulation d'une stratégie de rétablissement permet au réseau de reprendre son fonctionnement à partir d'un état connu.

7.3 Menaces contre la cybersécurité et méthode à suivre pour y remédier

Du point de vue X.800, les menaces visant un système de communication de données sont les suivantes:

a) destruction d'informations et/ou d'autres ressources;

b) corruption ou modification d'informations;

c) vol, suppression ou perte d'informations et/ou d'autres ressources;

d) divulgation d'informations; et

e) interruption de services.

D'après le document [UIT-T X.800], les menaces peuvent être accidentelles ou intentionnelles et peuvent être actives ou passives. Les menaces accidentelles sont celles pour lesquelles il n'y a pas de préméditation. Comme exemples de menaces accidentelles concrétisées, on peut citer les dysfonctionnements de système, les bourdes au niveau de l'exploitation et les bogues logiciels. Les menaces intentionnelles peuvent aller de l'examen occasionnel au moyen d'outils de surveillance disponibles facilement à des attaques sophistiquées fondées sur une connaissance particulière des systèmes. Si elle est concrétisée, une menace intentionnelle peut être considérée comme une "attaque". Les menaces passives sont celles pour lesquelles, si elles sont concrétisées, aucune information contenue dans le ou les systèmes ne serait modifiée et le fonctionnement et l'état du

système resteraient inchangés. Le recours à une écoute clandestine passive pour observer les informations transmises sur une ligne de communications constitue la concrétisation d'une menace passive. Les menaces actives contre un système font intervenir l'altération d'informations contenues dans le système ou des modifications de l'état ou du fonctionnement du système. Une modification malveillante des tables de routage d'un système par un utilisateur non autorisé est un exemple de menace active. L'Appendice I décrit brièvement quelques types particuliers d'attaques.

Les menaces contre la sécurité X.800 s'appliquent aussi au cyberenvironnement. D'après le document [UIT-T X.800], les fonctionnalités de sécurité ont tendance à accroître le coût d'un système et peuvent rendre son utilisation plus difficile. Avant de concevoir un système sûr, il est donc recommandé d'identifier les menaces spécifiques contre lesquelles une protection est nécessaire. C'est ce que l'on appelle l'évaluation des menaces. Les vulnérabilités d'un système sont nombreuses mais seules quelques-unes sont exploitables parce que les occasions d'attaque sont insuffisantes ou parce que le résultat ne justifie pas l'effort et le risque de détection. Les détails de l'évaluation des menaces sortent du cadre de la présente Recommandation, mais les grandes lignes de cette évaluation sont les suivantes:

Les menaces étant dirigées contre des actifs, la première étape consiste à dresser la liste des actifs à protéger. L'étape suivante de l'évaluation est une analyse des menaces, suivie par une analyse des vulnérabilités (y compris une évaluation des conséquences) puis la détermination des contre-mesures et des mécanismes de sécurité.

a) identifier les vulnérabilités du système;

b) analyser la probabilité pour que des menaces visent à exploiter ces vulnérabilités;

c) évaluer les conséquences qui résulteraient de la concrétisation de chaque menace;

d) estimer le coût de chaque attaque;

e) évaluer le coût des contre-mesures potentielles; et

f) choisir les mécanismes de sécurité qui sont justifiés (éventuellement sur la base d'une analyse de rentabilité).

Dans certains cas, des mesures non techniques (couverture d'assurance par exemple) peuvent constituer une alternative rentable aux mesures de sécurité techniques. En général, il est impossible d'assurer une sécurité technique parfaite. L'objectif devrait donc être de faire en sorte que le coût d'une attaque soit suffisamment élevé pour ramener le risque à des niveaux acceptables.

7.4 Sécurité des communications de bout en bout

Le document [UIT-T X.805] définit un cadre applicable à la sécurité de bout en bout des réseaux. Il s'applique à divers types de réseaux dans lesquels la sécurité de bout en bout est importante. L'architecture est indépendante de la technologie sous-jacente du réseau.

L'architecture de sécurité, dont l'objet est de résoudre les problèmes de sécurité mondiale auxquels les fournisseurs de services, les entreprises et les clients sont confrontés, s'applique aux réseaux vocaux, de données et intégrés, qu'ils soient sans fil, optiques ou filaires. Elle vise à répondre aux préoccupations de sécurité concernant la gestion, la commande et l'utilisation de l'infrastructure du réseau, des services et des applications. Le document [UIT-T X.805] permet de détecter et de réduire de façon proactive les vulnérabilités de sécurité pour les menaces connues. L'architecture de sécurité subdivise, sur le plan logique, un ensemble complexe de fonctionnalités de sécurité de réseau de bout en bout en composants architecturaux distincts. Grâce à cette subdivision, il est possible d'adopter une approche systématique de la sécurité de bout en bout, qui peut être utilisée pour envisager de nouvelles solutions de sécurité ainsi que pour évaluer la sécurité dans les réseaux existants.

Dans le document [UIT-T X.805], une dimension de sécurité est un ensemble de mesures de sécurité destinées à traiter un aspect particulier de la sécurité dans le réseau. Dans ce même

document, on définit huit dimensions destinées à assurer une protection contre toutes les principales menaces affectant la sécurité. Ces dimensions ne sont pas limitées au réseau, elles englobent aussi les applications et les informations d'utilisateur final. Les dimensions de sécurité s'appliquent aux fournisseurs de services ou aux entreprises qui offrent des services de sécurité à leurs clients. Ce sont:

1) le contrôle d'accès;
2) l'authentification;
3) la non-répudiation;
4) la confidentialité des données;
5) la sécurité des communications;
6) l'intégrité des données;
7) la disponibilité; et
8) le respect de la vie privée.

Pour définir une solution de sécurité de bout en bout, les dimensions de sécurité sont appliquées à une hiérarchie de groupes d'équipements et de fonctionnalités de réseau, appelés couches de sécurité. Les trois couches de sécurité suivantes sont examinées:

1) la couche de sécurité relative à l'infrastructure;
2) la couche de sécurité relative aux services; et
3) la couche de sécurité relative aux applications.

Les couches de sécurité désignent les aspects au niveau desquels la sécurité est prise en compte dans les produits et les solutions, en offrant une vue séquentielle de la sécurité dans le réseau. On peut par exemple commencer par examiner les vulnérabilités de sécurité dans la couche infrastructure, puis dans la couche services et enfin dans la couche applications. La Figure 7-4.1 illustre comment les dimensions de sécurité sont appliquées aux couches de sécurité afin de réduire les vulnérabilités qui existent dans chaque couche.

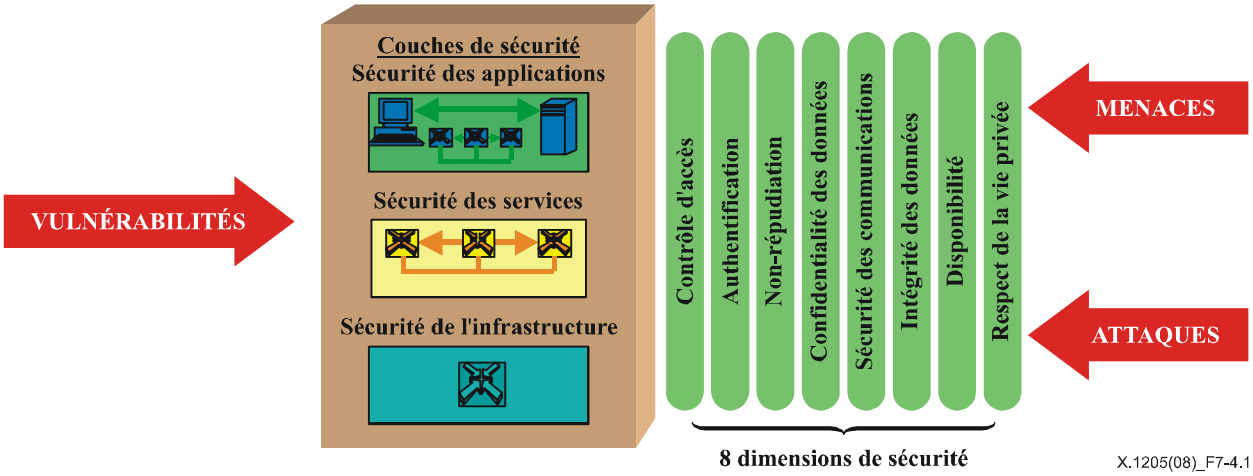

Figure 7-4.1 – Application des dimensions de sécurité aux couches de sécurité

Dans le document [UIT-T X.805], un plan de sécurité correspond à un certain type d'activités dans le réseau, protégées par les dimensions de sécurité. Dans ce même document, on définit trois plans de sécurité pour représenter les trois types d'activités protégées qui existent dans un réseau:

1) le plan de gestion;
2) le plan de commande; et

3) le plan d'utilisateur final.

Ces plans de sécurité visent à répondre aux besoins de sécurité particuliers associés respectivement aux activités de gestion du réseau, aux activités de commande ou de signalisation dans le réseau et aux activités d'utilisateur final. Dans le document [UIT-T X.805], il est proposé que les réseaux soient conçus de manière à ce que les événements concernant un seul plan de sécurité soient tenus à l'écart des autres plans de sécurité. Par exemple, de nombreuses consultations du système DNS au niveau du plan d'utilisateur final, résultant de demandes faites par des utilisateurs finals, ne devraient pas interdire l'utilisation de l'interface OAM&P dans le plan de gestion, pour qu'un administrateur puisse corriger le problème.

La Figure 7-4.2 illustre l'architecture de sécurité comportant les plans de sécurité. Le concept de plans de sécurité permet de faire une distinction entre les problèmes de sécurité propres aux différentes activités et de pouvoir les régler de façon indépendante. Prenons l'exemple d'un service de VoIP, qui relève de la couche de sécurité relative aux services: la sécurisation de la gestion du service devrait être indépendante de la sécurisation de la commande du service et indépendante de la sécurisation des données d'utilisateur final transportées par le service (par exemple les signaux vocaux de l'utilisateur).

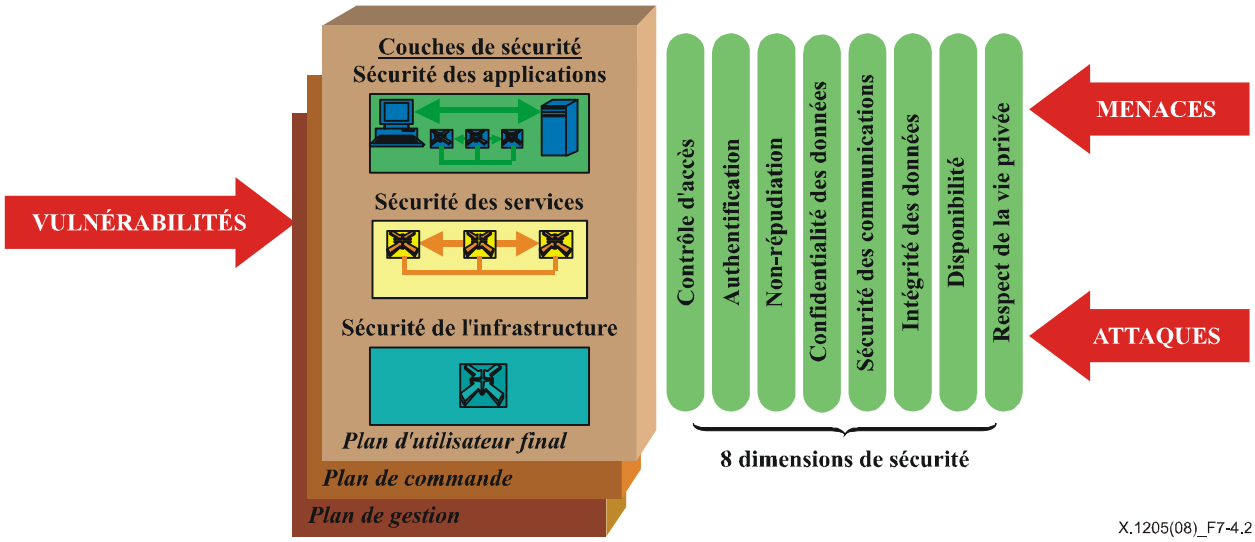

Figure 7-4.2 – Plans de sécurité correspondant aux différents types d'activités dans le réseau

8 Stratégies possibles de protection des réseaux

La sécurité est définie dans toutes les couches architecturales d'un réseau. Cette approche de la sécurité par couches offre un bon point de départ pour la conception de réseaux sécurisés. Elle permet à une couche supérieure de définir ses propres exigences de sécurité ainsi que d'utiliser les services de sécurité des couches inférieures. Elle permet de développer des solutions de sécurité souples et modulables au niveau du réseau, au niveau des applications et au niveau de la gestion pour toutes les organisations.

8.1 Gestion de politique en boucle fermée

Une politique de sécurité correctement conçue et mise en œuvre est une nécessité absolue pour tous les types d'entreprises et d'organisations. La politique de sécurité est généralement définie dans un document procédural vivant dont l'application, la mise en œuvre et la mise à jour suivent l'évolution de l'infrastructure de l'entreprise ou de l'organisation ainsi que des exigences de service.

La politique de sécurité identifie clairement les ressources de l'organisation (ou de l'entreprise) qui présentent des risques et les méthodes à appliquer en conséquence pour réduire les menaces. Elle prévoit la réalisation d'une évaluation des vulnérabilités et des risques et définit des règles de contrôle d'accès appropriées. L'évaluation des risques et des vulnérabilités est réalisée à tous les niveaux du réseau. Utile pour identifier et découvrir les atteintes à la sécurité, la politique établit les réactions indiquées face à ces atteintes.

Il est recommandé que les administrateurs des technologies de l'information et des réseaux utilisent des outils pour évaluer les vulnérabilités dans leurs réseaux. On applique le principe de l'accès avec les moindres privilèges. Entre autres tâches, les administrateurs des technologies de l'information et des réseaux doivent faire en sorte que les enregistrements d'audit soient analysés, ce qui permet de fermer la boucle en matière de gestion de politique. Si des problèmes sont relevés dans les audits, les administrateurs des technologies de l'information et des réseaux veillent à ce que la politique soit mise à jour afin de tenir compte des mesures révisées.

Une politique de sécurité qui n'est pas appliquée est inutile. L'application de la politique de sécurité dépend des personnes. Les responsabilités en matière d'application de la politique devraient être clairement établies.

8.2 Gestion d'accès uniforme

Le terme gestion d'accès est employé pour définir des systèmes qui peuvent recourir à la fois à des services d'authentification et d'autorisation afin de contrôler l'utilisation d'une ressource. L'authentification est le processus selon lequel un utilisateur ou une entité demande à un réseau l'établissement d'un identificateur. L'autorisation détermine le niveau de privilèges de cette entité sur la base du contrôle d'accès. Le contrôle du niveau d'accès est fondé sur la définition et l'application d'une politique de contrôle. La Figure 8-2 présente le modèle de référence pour une authentification et une autorisation sécurisées.

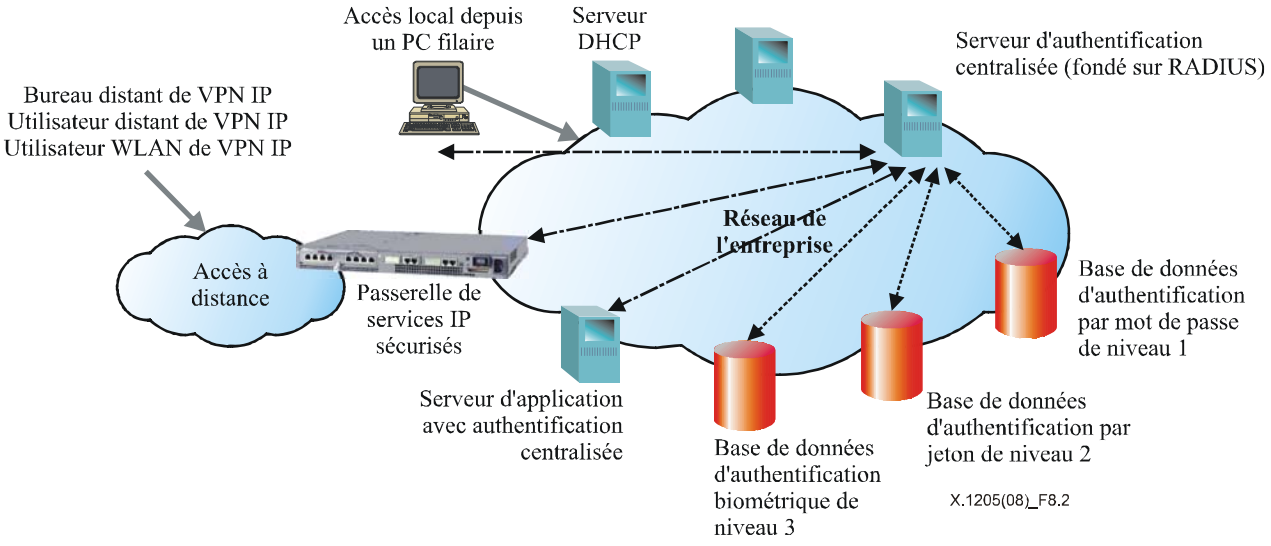

Figure 8-2 – Modèle de référence pour une authentification et une autorisation sécurisées

Il découle de la Figure 8-2 les recommandations suivantes:

1) Utilisation d'un mécanisme d'authentification centralisé afin de faciliter l'administration et de supprimer la nécessité d'un stockage local des mots de passe. (Les mots de passe stockés localement ont tendance à être statiques et faibles.)

2) Utilisation d'un système d'autorisation centralisé, étroitement couplé avec le système d'authentification, avec une granularité appropriée pour l'entreprise considérée.

3) Application de règles relatives à des mots de passe forts (complexes) pour tous les mots de passe.

4) Stockage sécurisé de tous les mots de passe dans un format de chiffrement irréversible (hachage).

5) Application du principe de simplicité afin de faciliter l'utilisation et l'administration. Un système simple est un système sûr étant donné que les mesures de protection ont beaucoup plus de chances d'être suivies.

6) Journalisation sécurisée de tous les événements liés à la sécurité en ce qui concerne l'authentification et l'autorisation.

Les méthodes de gestion d'accès comportent le filtrage en fonction de l'origine IP, les techniques fondées sur des proxys et les techniques fondées sur des justificatifs d'identité. Chaque méthode présente des avantages et des limites. Suivant le type d'entreprise et suivant l'entreprise même, plusieurs méthodes ou une combinaison de méthodes peuvent être utilisées. Par exemple, une entreprise peut choisir de gérer l'accès sur la base d'un filtrage en fonction de l'origine IP pour les stations de travail et peut choisir d'utiliser une technique fondée sur des justificatifs d'identité pour les autres utilisateurs.

Pour authentifier un utilisateur, on peut utiliser plusieurs méthodes, par exemple fondées sur des mots de passe, sur des mots de passe à usage unique, sur des techniques biométriques, sur des cartes à puce ou sur des certificats. L'authentification par mot de passe doit utiliser des mots de passe forts (comportant par exemple au moins huit caractères, avec au moins un caractère alphabétique, un caractère numérique et un caractère spécial). L'authentification par mot de passe seule peut être insuffisante. Sur la base d'une évaluation des vulnérabilités, il peut être nécessaire de combiner l'authentification par mot de passe avec d'autres méthodes d'authentification et d'autorisation, par exemple fondées sur des certificats, le protocole simple d'accès à l'annuaire (LDAP), le service d'authentification à distance des utilisateurs entrants (RADIUS), le protocole Kerberos et l'infrastructure de clé publique (PKI).

Tous les mécanismes d'authentification présentent des avantages et des inconvénients. Ceux qui sont fondés sur des combinaisons identité d'utilisateur/mot de passe sont simples, peu onéreux et faciles à gérer, mais il est très difficile pour les utilisateurs de retenir une multitude de mots de passe complexes. Les systèmes d'authentification à deux facteurs ou à trois facteurs assurent une authentification plus forte, mais tous sont onéreux, présentent une complexité supplémentaire et sont difficiles à gérer.

Un système "à mot de passe unique" dans lequel on applique des mots de passe forts peut être une bonne solution pour l'authentification et l'autorisation dans les entreprises. Il offre une grande sécurité d'authentification et une autorisation granulaire et il est plus facile à administrer. Dans un tel système, le mot de passe fort et unique de l'utilisateur est synchronisé avec bon nombre d'applications et de systèmes dans toute l'entreprise en vue de l'authentification et de l'autorisation. Pour les fonctions d'authentification et d'autorisation, l'ensemble des systèmes et des applications de l'entreprise renvoient automatiquement au système à mot de passe unique. Etant donné que les utilisateurs ont un seul mot de passe fort à retenir, le système est simple à utiliser et a peu de risques d'être contourné. Le système à mot de passe unique présente les avantages suivants:

- Une seule méthode cohérente pour l'établissement des mots de passe.
- Une seule méthode cohérente pour l'authentification et l'autorisation.
- Une seule méthode pour l'enregistrement et la clôture des comptes d'utilisateur.
- L'application de lignes directrices relatives aux mots de passe forts dans l'entreprise.
- La cohérence – les utilisateurs savent ce qu'ils doivent faire.

- Un système standard – facile à prendre en charge et à adopter.
- Un système rapide – interface standard et API.
- Des coûts peu élevés, peu d'appels d'assistance.

Les plus grandes difficultés pour l'entreprise ouverte et pour l'entreprise étendue résident dans la conception de leur politique de gestion d'accès. Il est utile de considérer la gestion d'accès comme une partie intégrante de la politique de sécurité. Ces organisations devraient concevoir un système de gestion d'accès uniforme avec des règles fines qui s'interface correctement avec:

- les annuaires et bases de données contenant des attributs d'identité;
- plusieurs systèmes d'authentification (mot de passe, Kerberos, TACACS et RADIUS);
- les hôtes, les applications et les serveurs d'application.

Le système de gestion d'accès uniforme devrait assurer une gestion de session pour chaque utilisateur après que celui-ci a été authentifié. Il est recommandé d'utiliser un système souple de configuration et d'application de politique avec des règles fines afin de pouvoir traiter des objets spécifiques. La surveillance et la comptabilité devraient être appropriées et les enregistrements d'audit devraient être sécurisés. Il est recommandé que les administrateurs aient chacun un compte unique et qu'ils puissent remonter aux individus pour la responsabilité des actions.

8.3 Communications sécurisées

Les réseaux unifiés peuvent acheminer des paquets vocaux, vidéo et de données. La sécurisation du trafic dans le réseau a pour objectif de garantir la confidentialité, l'intégrité et l'exactitude des communications dans le réseau. La sécurité devrait être assurée pour les appels et la signalisation dans les réseaux téléphoniques. Une technologie de chiffrement est utilisée pour les réseaux de données, vocaux et mobiles.

Pour le chiffrement, on peut utiliser:

- des techniques VPN avec IPSec, un en-tête d'authentification (AH) et une charge utile de sécurité encapsulante (ESP) ou une tunnellisation fondée sur le protocole de tunnellisation de couche 2 (L2TP);
- une gestion des clés fondée sur le protocole d'échange de clés Internet (IKE);
- une gestion des certificats fondée sur l'infrastructure de clé publique [b-UIT-T X.509] (PKIX);
- le protocole de gestion des certificats (CMP) (cf. [b-IETF RFC 2510]) et le protocole d'état de certificat en ligne (OCSP) (cf. [b-IETF RFC 4557]);
- dans la couche application, le protocole TLS (cf. [b-IETF RFC 4366]) avec des clés fortes.

Il est important d'utiliser des algorithmes de chiffrement et de hachage normalisés, par exemple DES, 3DES, AES, RSA et DSA (cf. [b-IETF RFC 2828]). On peut utiliser les algorithmes MD5 (cf. [b-IETF RFC 1321]) et SHA-1 (cf. [b-IETF RFC 3174]) pour l'intégrité des messages, et les algorithmes de Diffie-Hellman (cf. [b-IETF RFC 2631]) et RSA (cf. [b-IETF RFC 2828]) pour l'échange de clés.

NOTE – Le NIST (*National Institute of Standards and Technology*) incite maintenant à utiliser l'algorithme SHA-256 (algorithme de hachage sécurisé avec clés codées sur 256 bits) plutôt que l'algorithme SHA-1.

Le protocole de confidentialité équivalente à celle d'un réseau filaire (WEP), défini dans les normes [b-IEEE 802.11], définit une technique destinée à protéger la transmission hertzienne entre les points d'accès des réseaux locaux sans fil (WLAN) et les cartes d'interface de réseau (NIC). Ce protocole s'est avéré offrir un faible niveau de sécurité. Des mesures de protection supplémentaires comme IPSec sont nécessaires pour sécuriser le WLAN sur WEP. Une autre solution consiste à utiliser l'accès protégé Wi-Fi (WPA) pour assurer une protection supplémentaire.

8.4 Sécurité à profondeur variable

Un VLAN est un groupe de dispositifs de réseau tels que des serveurs et d'autres ressources de réseau, qui sont configurés pour se comporter comme s'ils étaient raccordés à un même segment de réseau. Dans chaque VLAN, les ressources et les serveurs des autres utilisateurs du réseau sont invisibles. Les VLAN contribuent au respect de la qualité de fonctionnement requise grâce à une segmentation plus efficace du réseau. Les VLAN limitent la dissémination du trafic de diffusion et du trafic entre nœuds, ce qui a pour effet de réduire le trafic extérieur acheminé dans le réseau. Dans les VLAN, tous les paquets acheminés d'un VLAN à un autre peuvent également passer par un routeur, des mesures de sécurité pouvant être mises en œuvre au niveau du routeur pour limiter l'accès au segment.

La sécurité par couches permet d'offrir une sécurité à profondeur variable. Chaque niveau de sécurité supplémentaire s'appuie sur les capacités de la couche inférieure et offre une sécurité de plus en plus fine.

Une compartimentalisation et une segmentation de base du réseau peuvent par exemple être assurées par des VLAN. Ainsi, diverses fonctions d'entreprises peuvent être contenues et segmentées dans des réseaux locaux privés, le trafic transversal provenant des autres segments VLAN étant contrôlé ou interdit. Le déploiement de VLAN dans les différents sites d'une organisation présente plusieurs avantages. Par exemple, l'utilisation d'étiquettes de VLAN permet de partager le trafic en différents groupes (par exemple finance, ressources humaines et ingénierie). Le partage des données sans "fuite" entre les VLAN est important pour la sécurité.

Une deuxième couche de sécurité peut être obtenue par l'utilisation de capacités de pare-feu/filtrage périmétriques et réparties au niveau des points stratégiques du réseau. La couche des pare-feu permet de segmenter encore le réseau en zones plus petites et permet d'établir des connexions sécurisées avec le réseau public. Les pare-feu limitent l'accès au trafic entrant et sortant aux protocoles qui sont explicitement configurés dans le pare-feu considéré. En outre, une capacité d'authentification pour les utilisateurs entrants ou sortants peut être prise en charge. Les pare-feu qui assurent la traduction d'adresse réseau (NAT) permettent d'optimiser l'adressage IP dans le réseau comme cela est spécifié dans le document [IETF RFC 1918] (attribution des adresses pour les réseaux privés interconnectés).

L'utilisation de pare-feu offre une couche supplémentaire de protection qui est utile pour le contrôle d'accès. L'application d'un accès fondé sur une politique permet d'adapter l'accès aux besoins de l'entreprise. L'adoption d'une solution avec des pare-feu répartis présente l'avantage supplémentaire de la modulabilité au fur et à mesure de l'évolution des besoins de l'entreprise. Des pare-feu personnels peuvent être déployés au niveau des systèmes d'extrémité afin de garantir l'intégrité des applications.

Des VPN de couche 3 peuvent être ajoutés en tant que troisième couche afin d'améliorer la sécurité. Les VPN permettent d'affiner le contrôle d'accès des utilisateurs et la personnalisation. Ils assurent une sécurité très fine jusqu'au niveau de l'utilisateur individuel et permettent d'offrir un accès à distance sécurisé aux sites distants et aux partenaires commerciaux. Avec les VPN, il n'est pas nécessaire d'utiliser des lignes spécialisées. L'utilisation d'un routage dynamique sur des tunnels sécurisés dans l'Internet constitue une solution hautement sécurisée, fiable et évolutive. L'utilisation de VPN conjointement avec l'utilisation de VLAN et de pare-feu permettent à l'administrateur de réseau de limiter l'accès par un utilisateur ou par un groupe d'utilisateurs sur la base de critères de politique et compte tenu des besoins de l'entreprise. Les VPN offrent une garantie plus forte d'intégrité et de confidentialité des données. Un chiffrement fort des données peut être mis en œuvre dans cette couche pour assurer la confidentialité et l'intégrité des données.

Les solutions de sécurité par couches sont souples et modulables. Elles peuvent être adaptées aux besoins de sécurité de l'entreprise.

8.5 Sécurisation de la gestion

Qu'il soit considéré comme une "pratique exemplaire" ou qu'il fasse partie intégrante de l'architecture de sécurité d'une organisation ou d'une entreprise, un canal ou un plan de gestion sécurisé sert de base à tous les autres éléments de gestion, de qualité de fonctionnement et de capacité de survie du réseau. La Figure 8-5 présente un modèle de référence possible pour la sécurisation de la gestion concernant le centre d'exploitation du réseau (NOC).

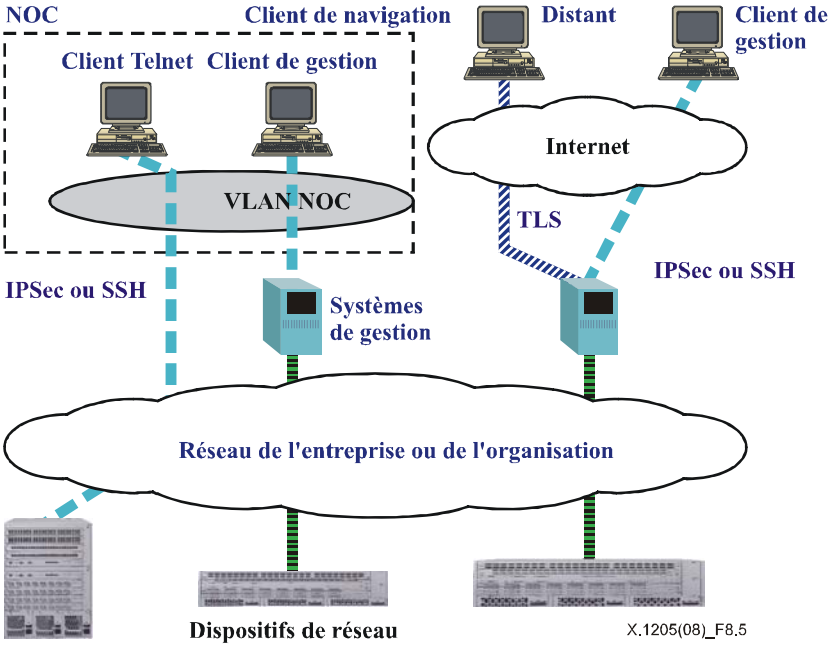

Figure 8-5 – Modèle de référence pour la sécurisation de la gestion

La gestion sécurisée est une approche globale et non une fonctionnalité de sécurité mise en œuvre dans un élément de réseau donné. C'est pourquoi l'approche recommandée dans la présente Recommandation englobe les zones critiques de l'infrastructure du réseau et inclut des mesures spécifiques pour réduire les menaces potentielles contre le réseau. Chacun des domaines ci-dessous représente un composant critique à prendre en considération du point de vue de la sécurité pour assurer une protection homogène autour du réseau.

Neuf domaines essentiels de gestion du réseau sont à prendre en considération du point de vue de la sécurité avant qu'un plan de gestion du réseau puisse être considéré comme étant sûr. Ces domaines sont les suivants:

- Journaux d'activités sécurisés
- Authentification des opérateurs de réseau
- Contrôle d'accès pour les opérateurs de réseau
- Chiffrement du trafic de gestion de réseau
- Accès à distance sécurisé pour les opérateurs
- Pare-feu
- Détection des intrusions
- Renforcement du système d'exploitation
- Absence de virus dans les logiciels.

8.5.1 Gestion de politique

On peut utiliser des journaux sécurisés pour conserver un enregistrement d'audit des activités des utilisateurs ou des administrateurs ainsi que des événements produits par le dispositif proprement dit, ce qui constitue un élément essentiel de fermeture de la boucle relative à la gestion de politique. Les données brutes collectées sont appelées "journal d'audit" et le cours vérifiable des événements dans les journaux d'audit est appelé "enregistrement d'audit". Pour être efficaces, les journaux d'audit de sécurité doivent contenir suffisamment d'informations pour l'examen ou l'analyse ultérieur des incidents de sécurité. Ces journaux d'audit permettent d'atteindre plusieurs objectifs liés à la sécurité, y compris la responsabilité individuelle, la reconstitution des événements passés, la détection des intrusions et l'analyse des problèmes. Les journaux peuvent aussi être utilisés pour l'analyse des tendances à long terme. Les informations contenues dans les journaux d'audit aident à identifier la cause profonde d'un problème de sécurité et à empêcher les incidents futurs; ces informations devraient être stockées de façon sécurisée. Les journaux d'audit peuvent par exemple être utilisés pour reconstituer la séquence des événements qui ont conduit à un problème, tel que l'accès non autorisé d'un intrus à des ressources de système, ou un dysfonctionnement du système dû à une configuration incorrecte ou à une mise en œuvre défectueuse.

8.5.2 Gestion d'accès sécurisée

L'authentification des opérateurs de réseau devrait être fondée sur une authentification centralisée forte des opérateurs et des administrateurs de réseau. L'administration centralisée des mots de passe permet d'appliquer des mots de passe forts et supprime la nécessité d'un stockage local des mots de passe au niveau des éléments de réseau et des systèmes EMS. Le protocole RADIUS est le mécanisme tout désigné pour automatiser l'authentification centralisée.

Il convient d'utiliser une bonne pratique en ce qui concerne le contrôle d'accès pour les opérateurs de réseau. Par exemple, pour déterminer le niveau d'autorisation, on peut utiliser des techniques fondées sur des serveurs RADIUS pour offrir un niveau de contrôle d'accès de base et utiliser en plus un serveur LDAP pour assurer un contrôle d'accès plus fin en cas de besoin.

8.5.3 Chiffrement du trafic de gestion de réseau

Le chiffrement est recommandé pour l'ensemble du trafic de données utilisé dans une capacité de gestion de réseau pour garantir la confidentialité et l'intégrité des données. Les entreprises utilisent de plus en plus une gestion de réseau dans la bande, de sorte qu'il est nécessaire de séparer le trafic de gestion par le biais du chiffrement. Le chiffrement du trafic de gestion offre un niveau élevé de protection contre les utilisateurs internes à l'exception du petit groupe de ceux qui disposent d'un accès légitime aux clés de chiffrement. Il convient de prévoir un chiffrement entre les clients de type centre d'exploitation du réseau (NOC) et les serveurs de type système de gestion d'élément (EMS) et/ou les éléments de réseau. Le trafic SNMP est visé, car il existe des vulnérabilités connues avec les versions 1 et 2 du protocole SNMP, qui sont résolues dans la version 3 du protocole SNMP. Suivant le type de trafic, les protocoles de sécurité à utiliser pour ces liaisons sont TLS, IPSec et SSH (cf. [b-IETF RFC 4252]). Le protocole SSH est un protocole de sécurité au niveau de l'application, qui remplace directement les protocoles Telnet (cf. [b-IETF RFC 854]) et FTP (cf. [b-IETF RFC 959]), mais qui ne peut en principe pas être utilisé pour protéger d'autres types de trafic. Quant au protocole IPSec, il s'applique entre la couche réseau (couche 3) et la couche transport (couche 4) et peut être utilisé pour protéger n'importe quel type de trafic de données indépendamment des applications et des protocoles utilisés. Il convient d'utiliser de préférence le protocole IPSec mais le protocole SSH peut être utilisé si le trafic est uniquement de type Telnet et FTP. La technologie TLS permet de protéger le trafic HTTP lorsque ce type de trafic est utilisé dans une capacité de gestion de réseau entre des clients NOC et les systèmes EMS et/ou les éléments de réseau. Un dispositif VPN IPSec externe peut être utilisé dans diverses parties du réseau pour sécuriser le trafic de gestion.

8.5.4 Accès à distance sécurisé pour les opérateurs

La sécurité doit être assurée pour les opérateurs et les administrateurs qui gèrent le réseau depuis un emplacement distant sur un réseau public. La solution préférée consiste à mettre en place un réseau privé virtuel sécurisé fondé sur IPSec, étant donné qu'elle offrira un chiffrement fort et l'authentification de tous les opérateurs distants. Par exemple, un produit VPN pourrait être installé au niveau de l'interface du système de gestion et tous les opérateurs devraient être équipés de clients d'accès extranet pour leurs ordinateurs portables ou stations de travail.

8.5.5 Pare-feu

Pour appliquer les principes de sécurité à profondeur variable, une bonne pratique consiste à segmenter l'environnement de gestion du réseau au moyen de VLAN et de pare-feu. Le pare-feu contrôle le type (protocole, numéro de port, adresse d'origine et adresse de destination) de trafic utilisé pour passer la frontière entre différents domaines de sécurité. Suivant son type (filtrage en fonction de l'application ou filtrage des paquets), le pare-feu peut aussi servir à filtrer le contenu du flux de données concernant les applications. L'emplacement, le type et les règles de filtrage des pare-feu sont propres à chaque mise en œuvre de réseau.

8.5.6 Détection des intrusions

Des systèmes de détection des intrusions fondés sur des hôtes peuvent être intégrés dans les serveurs de gestion pour assurer la protection contre les intrusions dans le réseau. Les systèmes de détection des intrusions peuvent être utilisés pour avertir les administrateurs de réseau de la possibilité d'un incident de sécurité (par exemple une atteinte à un serveur ou une attaque par déni de service).

8.5.7 Couche de sécurité relative aux applications

Il est recommandé de renforcer tous les systèmes d'exploitation utilisés dans la capacité de gestion de réseau, aussi bien les systèmes d'exploitation généraux que les systèmes d'exploitation en temps réel intégrés. Pour les systèmes d'exploitation pour lesquels il n'existe pas de guide spécifique de renforcement, il convient de consulter le fabricant pour obtenir les dernières procédures et les derniers correctifs pour le renforcement.

8.5.8 Absence de virus dans les logiciels

Il faut examiner tous les logiciels, développés en interne ou achetés à un tiers, et faire en sorte qu'ils ne contiennent pas de virus dans la mesure du raisonnable. Il faut élaborer une procédure de recherche des virus, dans laquelle tous les logiciels seront analysés au moyen d'un outil spécifié de détection des virus avant d'être incorporés dans un produit.

8.6 Sécurité par couches: application, réseau et gestion de réseau

Chaque organisation ou entreprise a un seuil de sécurité différent et une infrastructure technique différente. Les applications sur Internet représentent des risques et des menaces accrus pour l'entreprise. Elles peuvent donc avoir une sécurité intégrée au niveau application. Quoi qu'il en soit, l'utilisation de la fonctionnalité de sécurité qui peut être assurée par les couches de réseau inférieures améliore la sécurité de ces applications.

Il est recommandé aux entreprises présentes sur l'Internet de concevoir leurs sites avec une précaution extrême. Le document [b-IETF RFC 2196] (manuel sur la sécurité des sites) constitue une bonne référence sur la sécurité des sites. Au niveau application, il est recommandé d'utiliser une politique de sécurité fine. Lorsque c'est possible, les objets devraient être adressables à partir d'identificateurs universels de ressource (URI). Il convient de désactiver les fonctionnalités inutiles. Lorsque c'est possible, il convient d'utiliser le protocole TLS. Il est recommandé d'utiliser des passerelles au niveau application et de prévoir une authentification et une autorisation fortes. Lorsque l'infrastructure de sécurité le permet, il convient de sécuriser les services de messagerie

électronique au moyen de S/MIME (cf. [b-IETF RFC 2311]) et de techniques telles que PGP (cf. [b-IETF RFC 1991]).

Dans la couche réseau, il est recommandé d'utiliser les techniques examinées au § 8.7 pour garantir une sécurité acceptable pour l'entreprise. La sécurité est obtenue dans le cadre d'une architecture en couches qui peut être adaptée en fonction des besoins de sécurité de chaque type d'entreprise.

La sécurisation du trafic de gestion de réseau est un élément essentiel de la sécurisation du réseau. Pour cela, on peut commencer par garantir le renforcement du système d'exploitation contre les menaces connues. Il convient de consulter le fabricant du système d'exploitation pour obtenir les dernières procédures et les derniers correctifs pour le renforcement. Il convient de procéder pas à pas pour vérifier l'absence de virus connus dans tous les logiciels qui sont installés. Il est préférable de toujours chiffrer l'ensemble du trafic de gestion au moyen du protocole IPSec ou TLS pour protéger le trafic HTTP. Il est recommandé de recourir au chiffrement si le trafic est acheminé en dehors du réseau local. Il est recommandé d'utiliser les protocoles SNMPv3 et RADIUS pour le contrôle d'accès à distance pour les opérateurs de réseau, avec des mécanismes de contrôle à plusieurs niveaux, comportant notamment l'utilisation de mots de passe forts, et il est préférable de prévoir une administration centralisée du système de contrôle d'accès. Des journaux sécurisés sont essentiels pour la journalisation du trafic de gestion de réseau.

8.7 Capacité de survie du réseau même en cas d'attaque

Dans l'environnement actuel, le réseau d'une entreprise prend en charge des opérations essentielles à l'exécution de la mission de l'entreprise et il est indispensable à la conduite de ses activités. Il est supposé être sécurisé, fiable et disponible pour les partenaires commerciaux en permanence.

De nombreuses techniques peuvent être utilisées pour garantir la fiabilité du réseau, autrement dit pour garantir le fonctionnement correct du réseau en cas de défaillance de composants logiciels et/ou matériels. Toutefois, lorsque des menaces de sécurité sont présentes, le modèle à utiliser est celui des réseaux avec capacité de survie. Un réseau doté d'une capacité de survie est un réseau qui continue à remplir un ensemble minimal de fonctionnalités essentielles en temps voulu en présence d'attaques. Les fonctionnalités essentielles consistent à fournir en temps voulu les services essentiels même si des parties du réseau sont inaccessibles ou défaillantes en raison d'une attaque.

Pour concevoir un réseau doté d'une capacité de survie, il faut commencer par classer les services de réseau en deux catégories, à savoir les services essentiels et les services non essentiels. La capacité de survie signifie qu'un réseau peut résister à une attaque. Il faut disposer d'une stratégie claire concernant le traitement d'une attaque et le rétablissement. Suivant le type d'attaque, il existe plusieurs stratégies possibles de résistance, d'identification et de rétablissement que l'administrateur de réseau souhaitera peut-être envisager. Un réseau doté d'une capacité de survie présente la particularité d'être adaptable. Par exemple, il peut rerouter le trafic vers un deuxième serveur si une intrusion ou une attaque est détectée sur le premier serveur.

Pendant la phase de conception de la politique de sécurité, il est nécessaire de déterminer les services essentiels qu'un réseau devrait pouvoir fournir même en cas d'attaque. Pendant cette phase, on détermine comment un réseau résistera à une attaque et comment il la surmontera et on définit la meilleure solution de rétablissement après une telle attaque. Qu'il s'agisse des systèmes de gestion, des hôtes, des applications, des routeurs ou des commutateurs, tous sont à prendre en considération dans l'analyse.

L'utilisation de mécanismes de contrôle d'accès avec une authentification et un chiffrement forts permet à un réseau doté d'une capacité de survie d'être plus résistant aux attaques. L'utilisation d'un filtrage des messages et des paquets ainsi que d'une segmentation du réseau et des serveurs permet aussi d'améliorer cette résistance. L'utilisation de techniques appropriées de détection des intrusions peut faciliter l'identification des attaques. Des techniques de secours appropriées peuvent être utilisées pour le rétablissement des systèmes et du réseau.

Appendice I

Techniques d'attaque

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

Le présent appendice décrit brièvement certaines des attaques qui posent particulièrement problème dans un environnement de traitement de données et de communication de données.

I.1 Description des menaces contre la sécurité

Il est conseillé aux professionnels des technologies de l'information de considérer leur réseau comme une ressource à laquelle accèdent des utilisateurs auxquels, d'une manière générale, on ne peut pas faire confiance. Les attaquants disposent d'une multitude d'outils, de techniques et de méthodes pour porter atteinte à un réseau. Les pirates peuvent employer ces outils pour lancer des attaques à plusieurs niveaux afin d'accéder au réseau. Dans certains cas, l'attaquant exploitera une atteinte à la sécurité puis lancera des attaques secondaires pour exploiter d'autres parties du réseau.

Le présent paragraphe décrit les techniques, outils et méthodes employés par les attaquants, les pirates et les intrus pour porter atteinte à un réseau.

I.1.1 Menaces d'accès non autorisé

L'accès non autorisé à des ressources de réseau résulte généralement d'une configuration incorrecte du système et de mauvaises utilisations. Un attaquant peut obtenir un accès illégal en tirant parti d'une authentification et d'une autorisation insuffisantes des utilisateurs et des tâches dans les systèmes d'entreprise, ou de pratiques manquant de rigueur de la part des employés (par exemple le postage de mots de passe, lorsque l'utilisateur est obligé de retenir plusieurs mots de passe).

Des pratiques comme l'attribution incorrecte de l'espace caché ou le partage de privilèges entre applications peuvent être à l'origine de graves vulnérabilités. Des attaques par porte dérobée peuvent être utilisées pour obtenir un accès non autorisé. Par exemple, un attaquant peut utiliser un dictionnaire de chaînes courantes pour deviner des noms d'utilisateur et des mots de passe et obtenir ainsi un accès non autorisé. Des mots de passe peuvent être obtenus par des moyens algorithmiques, ou peuvent être saisis en transit s'ils sont envoyés en clair.

Après avoir deviné un nom d'utilisateur et le mot de passe associé, l'attaquant dispose d'un accès aux ressources de l'organisation. Le niveau d'accès dépend des privilèges associés au compte compromis. L'ampleur des dommages que l'attaquant inflige à l'organisation dépend de ses intentions. Dans la plupart des cas, les pirates utiliseront le compte compromis pour installer une porte dérobée dans le réseau de l'entreprise.

Les protocoles d'accès à distance à la messagerie électronique tels qu'IMAP, POP3 et POP2, qui reposent sur des techniques simples d'authentification par nom d'utilisateur et mot de passe, peuvent être utilisés pour faciliter les attaques par force brute. Il existe des méthodes publiées qui permettent aux attaquants d'exploiter à distance les services de ces protocoles.

Il existe des méthodes encore plus sophistiquées pour obtenir un accès non autorisé. Des vers peuvent être utilisés pour lancer des attaques par usurpation d'identité à l'intérieur d'un système, dans lesquelles un composant de système usurpe l'identité d'un autre. Par exemple, des vers peuvent exploiter les flux dans l'option debug de sendmail et dans .rhosts (utilisés par exemple dans le système UNIX) en raison d'une authentification faible. L'option debug de sendmail peut être désactivée. Le maintien de cette option en position activée est un exemple de mauvaise utilisation.

I.1.2 Usurpation d'adresse IP

L'usurpation d'adresse IP constitue une attaque complexe qui exploite les relations de confiance. Employant des techniques d'usurpation d'identité, l'attaquant usurpe les identificateurs d'un hôte pour porter atteinte à sa sécurité. Cet hôte pense qu'il est en conversation avec un hôte de confiance.

Dans cet assaut, l'attaquant commence par identifier un hôte de confiance dont il va usurper l'identificateur. Pour cela, il peut d'abord déterminer les séquences de confiance pour l'hôte. Il s'agit généralement de déterminer la plage d'adresses IP à laquelle l'hôte fait confiance. L'étape suivante consiste à désactiver l'hôte, étant donné que l'attaquant va usurper ses identificateurs. Pour cela, l'attaquant peut employer des techniques telles que les attaques par inondation SYN TCP.

Les attaques par usurpation d'adresse IP peuvent réussir en raison de la falsification aisée des adresses IP et des limitations des techniques d'authentification d'adresse fondées sur le réseau. Ces attaques sont aveugles car il est possible que l'attaquant n'ait pas accès aux réponses envoyées par l'hôte visé. Toutefois, l'attaquant peut obtenir une communication bidirectionnelle si les tables de routage sont manipulées afin d'utiliser l'adresse IP d'origine usurpée. Les attaques par usurpation d'adresse IP sont souvent utilisées comme une première étape pour d'autres assauts (par exemple des attaques par déni de service (DoS) ou par inondation).

Il est toutefois à noter que la plupart des fournisseurs d'accès à l'Internet (mais certainement pas tous) et bon nombre des réseaux d'entreprise de grande envergure procèdent maintenant à un filtrage en fonction de l'adresse de sortie, ce qui empêche les attaques directes par usurpation d'adresse IP. Cela étant, les attaquants s'emploient à accumuler des "machines zombies" afin de conserver leur anonymat.

I.1.3 Renifleurs de réseau

Au départ, les renifleurs de réseau ont été conçus comme un outil permettant d'aider les gestionnaires de réseau à diagnostiquer les problèmes, à réaliser des analyses et à améliorer la qualité de fonctionnement de leurs réseaux. Ils opèrent dans un segment de réseau qui n'est pas commuté (par exemple les segments qui sont connectés par le biais d'un pivot) et peuvent ainsi voir l'ensemble du trafic sur ce segment.

Les anciens renifleurs lisaient les en-têtes des paquets circulant dans le réseau et se limitaient à déterminer les caractéristiques de paquet de bas niveau telles que l'adresse d'origine et l'adresse de destination. Quant aux renifleurs actuels, ils peuvent décoder les données des paquets relevant de toutes les couches du modèle OSI.

Les attaquants peuvent utiliser des renifleurs pour obtenir des informations relatives aux utilisateurs et des mots de passe à partir des paquets circulant dans les réseaux publics ou privés. L'utilisation de renifleurs peut permettre aux attaquants d'obtenir des informations précieuses concernant les noms d'utilisateur et les mots de passe, en particulier à partir d'applications comme FTP ou telnet qui envoient des mots de passe en clair. Les protocoles d'accès à distance à la messagerie électronique tels qu'IMAP, POP3 et POP2, qui reposent sur des techniques simples d'authentification par nom d'utilisateur et mot de passe, sont susceptibles de faire l'objet d'attaques par reniflage.

Etant donné que les utilisateurs ont tendance à réutiliser des mots de passe dans plusieurs applications et plates-formes, les attaquants peuvent utiliser les informations acquises pour obtenir un accès à diverses ressources sur le réseau, auquel cas la confidentialité de ces ressources risque d'être compromise. De plus, ces ressources peuvent aussi servir de base pour lancer d'autres attaques.

Les attaquants parviennent généralement à utiliser des renifleurs de réseau en portant atteinte à la sécurité physique de l'entreprise. Autrement dit, une personne se promène dans l'entreprise et connecte son ordinateur portable au réseau. Les risques s'appliquent aussi aux réseaux sans fil: dans ce cas, une personne se trouvant sur le parking peut obtenir un accès au réseau local de l'entreprise.

L'obtention d'un accès au réseau central par paquets permet à l'attaquant de déterminer les configurations et les modes de fonctionnement à exploiter ultérieurement.

I.1.4 Déni de service

Les attaques par déni de service (DoS) visent à empêcher les utilisateurs légitimes d'un service de pouvoir utiliser le service. Elles sont faciles à mettre en œuvre et peuvent causer des dommages importants. Elles peuvent provoquer une interruption du fonctionnement de l'entreprise et une déconnexion effective par rapport au reste du monde. Les attaques par déni de service réparti utilisent les ressources de plusieurs machines pour lancer des attaques DoS synchronisées sur une ressource.

Les attaques DoS peuvent prendre diverses formes et viser divers services. Elles ont pour but d'épuiser les ressources de réseau, de serveur, d'hôte et d'application et, pour certaines, d'interrompre la connectivité du réseau. Par exemple, une attaque par inondation SYN utilise des fausses demandes de connexion TCP semi-ouverte, qui épuisent la capacité mémoire de la ressource visée. Ces attaques peuvent empêcher les utilisateurs légitimes d'accéder à des hôtes, à des applications web ou à d'autres ressources de réseau. Elles peuvent entraîner:

- un refus de la connectivité du réseau à l'Internet;
- un refus de mettre des éléments de réseau à la disposition des utilisateurs légitimes;
- un refus de mettre des applications à la disposition des utilisateurs légitimes.

Les attaques DoS exploitent les faiblesses de l'architecture du système attaqué. Dans certains cas, elles exploitent la faiblesse de nombreux protocoles Internet courants, comme le protocole de message de contrôle sur Internet (ICMP). Par exemple, certaines attaques DoS consistent à envoyer un grand nombre de paquets écho (ping) ICMP à une adresse de diffusion IP. Les paquets utilisent une adresse IP usurpée d'une cible potentielle. Les réponses revenant à la cible peuvent la paralyser. On parle d'attaques par réflexion (smurf). Une autre forme d'attaque utilise des paquets UDP mais fonctionne selon le même principe.

I.1.5 Attaques par intercepteur

Dans ce type d'assaut, l'attaquant intercepte les messages d'échange de clé publique entre un serveur et un client. Il retransmet ces messages après avoir remplacé la clé demandée par sa clé publique. Les participants initiaux penseront qu'ils communiquent entre eux. L'attaquant peut simplement accéder aux messages ou peut les modifier. Des renifleurs de réseau peuvent être utilisés pour lancer de telles attaques.

I.1.6 Portes dérobées

Les portes dérobées sont des méthodes rapides d'accès aux ressources de réseau qui peuvent:

- avoir été mises en place délibérément par des développeurs de système pour permettre un accès rapide pendant le développement et qui n'ont pas été désactivées une fois le développement terminé;
- avoir été mises en place par des employés pour faciliter l'exécution de leurs tâches;
- faire partie des installations standard du système d'exploitation, qui n'ont pas été éliminées par le renforcement (par exemple combinaisons identité d'utilisateur et mot de passe par défaut);
- être mises en place par des employés mécontents pour permettre un accès après leur cessation d'emploi;
- avoir été créées par l'exécution d'un code malveillant (par exemple des virus).

I.1.7 Usurpation d'identité

Cela consiste à prétendre faire partie du personnel de maintenance ou d'ingénierie afin d'accéder au réseau. Il s'agit juste de la pointe de l'iceberg d'une variété de menaces qui sont fondées sur les brèches de la sécurité physique et les vulnérabilités humaines. Par exemple, un intrus peut modifier des données relatives à la gestion de la configuration et aux couches de signalisation du réseau ainsi que des données de facturation et d'utilisation.

I.1.8 Attaques par répétition

Ce type d'attaque se produit lorsqu'un message, ou une partie d'un message, est répété pour produire un effet non autorisé. Par exemple, une entité répète un message valable contenant des informations d'authentification pour s'authentifier elle-même.

I.1.9 Modification de messages

La modification d'un message a lieu lorsque le contenu d'une transmission de données est altéré sans détection et conduit à un effet non autorisé.

I.1.10 Attaques par des personnes internes

Ce type d'attaque se produit lorsque des utilisateurs légitimes d'un système se comportent de façon non prévue ou non autorisée. Bon nombre des délits informatiques connus font intervenir des personnes internes qui portent atteinte à la sécurité du système. Une sélection minutieuse du personnel et une sécurisation permanente des matériels, des logiciels et de la politique de sécurité peuvent contribuer à réduire les risques d'attaque par des personnes internes. Le fait de disposer de bons enregistrements d'audit pour augmenter la probabilité de détecter ce type d'attaque constitue également une bonne pratique à suivre.

I.2 Menaces contre la sécurité

Tous les types d'organisations (par exemple les entreprises) sont confrontés à une grande variété de menaces. Les besoins de sécurité et la stratégie de sécurité recommandée varient d'une organisation à l'autre. L'environnement le plus exigeant du point de vue de la sécurité est celui de l'entreprise ouverte. Dans ce cas, il faut envisager la sécurité de façon globale dans l'entreprise afin de contrôler l'accès des employés, des partenaires et même des clients aux bases de données et applications de l'entreprise.

I.2.1 Attaques dans la couche application

Les attaques dans la couche application peuvent prendre diverses formes et utiliser diverses méthodes. Etant donné que les hôtes web sont accessibles par le grand public à des adresses de port connues telles que spécifiées par des protocoles comme le protocole HTTP (port 80), les pirates peuvent se servir de cette connaissance pour lancer des attaques qui sont capables de contourner les pare-feu.

Les attaques dans la couche application exploitent les vulnérabilités présentes dans le système d'exploitation et dans les applications afin d'accéder aux ressources. Une configuration et une autorisation incorrectes peuvent provoquer des brèches dans la sécurité. Par exemple, un hôte pourrait être un serveur web et devrait fournir les pages web demandées à quiconque en fait la demande. La politique de sécurité pourrait spécifier que l'accès aux commandes des systèmes essentiels est limité par les hôtes aux administrateurs autorisés.

La récolte de comptes vise le processus d'authentification lorsqu'une application demande une identité d'utilisateur et un mot de passe. Les applications qui produisent des messages d'erreur différents lorsque l'identité d'utilisateur est incorrecte et lorsque le mot de passe est incorrect sont vulnérables à ce type d'attaque. Compte tenu du type de message d'erreur, un intrus peut lancer une attaque destinée à déterminer d'abord une identité d'utilisateur valable puis il utilise une technique de craquage de mots de passe pour obtenir le mot de passe.

Les attaques dans la couche application peuvent notamment être fondées sur des virus, des vers, une surcharge de la mémoire tampon ou une récolte de mots de passe. La mise en place de services web et de techniques d'identification unique ne fait qu'aggraver le problème, étant donné que, de ce fait, les applications existantes ont tendance à être installées sur le web. Lorsque ces applications ont été conçues, la sécurité et la connectivité web n'ont pas été prises en compte.

Certaines attaques dans la couche application ont simplement pour objectif de démanteler un site web. D'autres attaques visent à corrompre les témoins (cookies) d'un site web pour obtenir de façon illégitime des informations concernant un serveur particulier. En général, les applications ne vérifient pas la validité des cookies et peuvent devenir les victimes de l'exécution d'un code malveillant qui est caché dans les cookies. Dans les navigateurs actuels, il existe des vulnérabilités connues susceptibles de conduire à des attaques fondées sur les cookies.

Un attaquant peut aussi utiliser la technique du *cross-site scripting* afin d'insérer un code malveillant sous la forme d'une balise script qui est ajoutée à une adresse URL. Le code sera exécuté lorsqu'un utilisateur peu méfiant cliquera sur cette adresse URL. L'utilisation du protocole TLS permet de résoudre certains des problèmes de sécurité au niveau de la couche application. Toutefois, le protocole SSL ne protège pas complètement les applications web. Des attaques comme la récolte de comptes ou le craquage de mots de passe peuvent continuer à être lancées même si le protocole SSL est utilisé.

Pour réduire les menaces d'attaques dans la couche application, il est recommandé de renforcer tous les systèmes d'exploitation utilisés dans une capacité de gestion de réseau, aussi bien les systèmes d'exploitation généraux que les systèmes d'exploitation en temps réel intégrés. Il convient de suivre les guides spécifiques de renforcement à jour fournis par les fabricants. Pour certains systèmes existants utilisant d'anciens systèmes d'exploitation, il se peut qu'aucun correctif de sécurité ne soit fourni par le fabricant. Il est également recommandé d'utiliser une messagerie électronique sécurisée, des pare-feu au niveau de la couche application, des systèmes de prévention et de détection des intrusions dans les hôtes, des techniques d'authentification forte, des mots de passe forts et une commande de sortie appropriée dans les sites web afin d'interdire l'affichage de modifications non autorisées du contenu web.

I.2.2 Menaces dans la couche réseau

Un attaquant peut utiliser des outils courants pour lancer des attaques plus ou moins graves dans la couche réseau. Les entreprises étendues et les entreprises ouvertes sont particulièrement vulnérables aux attaques dans la couche réseau. Un certain nombre de menaces de sécurité graves sont généralement associées à l'infrastructure de réseau. Ces menaces incluent le sabotage, le vandalisme, la mauvaise configuration des systèmes ainsi que le déni de service, la surveillance du trafic, l'espionnage industriel et le vol de service. Les attaques peuvent être lancées depuis l'intérieur du réseau par des personnes internes ou par des sources externes (par exemple des pirates).

Des développements techniques récents en matière de piratage tels que les analyseurs de port fondés sur les terminaux mobiles montrent que les attaques visant l'infrastructure de réseau peuvent aussi provenir d'un terminal mobile. Il est recommandé de concevoir une bonne politique de sécurité et un processus de sécurité bien compris afin de protéger l'infrastructure de réseau. Les commutateurs, les routeurs, les points d'accès, les serveurs d'accès à distance, les points d'accès sans fil, les hôtes et les autres ressources font partie des actifs à protéger.

Les menaces et vulnérabilités affectant l'infrastructure de réseau qui sont généralement rencontrées dans les réseaux par paquets IP sont les suivantes:

1) Prolifération de protocoles peu fiables: certains réseaux continuent à utiliser des protocoles qui sont connus pour présenter des vulnérabilités de sécurité (ICMP, TELNET, SNMPv1&2, DHCP, TFTP, RIPv1, NTP, DNS et HTTP).

2) Utilisation de mots de passe statiques faibles, gérés localement: certains réseaux continuent à autoriser l'utilisation de mots de passe faibles qui sont fondés sur des mots courants du dictionnaire constitués de peu de lettres, qui sont faciles à deviner. Certains administrateurs peuvent utiliser un seul mot de passe dans tous les éléments de réseau, qui peut être partagé et est en principe connu de tous les administrateurs.

3) Informations relatives à la sécurité non protégées: dans certains réseaux, des informations essentielles (par exemple des fichiers de mots de passe) ne sont pas chiffrées. D'autres informations (par exemple des mots de passe) sont envoyées en clair dans le réseau. Les ensembles de règles applicables aux pare-feu sont mal définies et des clés cryptographiques faibles sont employées.

4) Chargement de logiciels et de fichiers de configuration non authentifiés: des menaces contre les réseaux peuvent provenir du chargement de logiciels ou de fichiers de configuration incorrects ou malveillants, qui peuvent entraîner une perte de service et conduire à des performances médiocres. Cette pratique conduit à l'ouverture de brèches dans la sécurité (par exemple installation de chevaux de Troie ou d'autres codes malveillants par des personnes internes ou externes). Elle conduit aussi à des configurations incorrectes sur les dispositifs.

5) Eléments de réseau et systèmes d'exploitation non renforcés: des menaces contre les réseaux peuvent résulter du chargement de systèmes d'exploitation par défaut auprès de fabricants, qui ne sont pas renforcés contre les attaques courantes (par exemple exécution de services inutiles, avec des comptes et des mots de passe par défaut laissés activés).

6) Ports et interfaces de gestion inutilement exposés au réseau public: des menaces contre les réseaux peuvent provenir d'interfaces de gestion dans la bande qui sont laissées accessibles sur l'Internet public. D'autres menaces peuvent être dues à un abus de mécanismes supports (par exemple accès au réseau central en mode support via une connexion commutée, RNIS ou autre).

I.2.3 Accès non autorisé

L'accès non autorisé renvoie à un certain nombre d'attaques de différents types. Le but ultime de l'attaquant est d'accéder de façon illégitime à certaines ressources. Il s'agit d'un problème de sécurité pour tous les types d'entreprise. Toute entreprise offrant un accès à l'Internet ou des capacités d'accès depuis un réseau local distant est susceptible de subir des attaques par accès non autorisé.

Les services d'accès à distance qui permettent aux employés en déplacement d'accéder à la messagerie électronique par le réseau commuté, les bureaux distants raccordés par des lignes commutées, les intranets et les extranets qui raccordent des parties externes au réseau de l'entreprise peuvent avoir pour conséquence une vulnérabilité du réseau au piratage, aux virus et à d'autres attaques. Les pirates peuvent utiliser des outils courants pour obtenir un accès au réseau de l'entreprise et peuvent alors compromettre des informations sensibles ou peuvent utiliser le réseau pour lancer des attaques contre d'autres réseaux.

Protéger le réseau à divers niveaux permet de faciliter la lutte contre l'accès non autorisé. Au niveau de la couche réseau, le recours à des pare-feu, à des serveurs proxy et à un filtrage des utilisateurs participant à une session permet de renforcer la protection, même si les pirates semblent toujours plus futés. Le recours à un contrôle d'accès des utilisateurs au niveau du réseau et de l'application avec une authentification et une autorisation appropriées permet aussi de réduire les risques d'accès non autorisé.

I.2.4 Ecoute clandestine

L'écoute clandestine est une menace difficile à détecter. Ici, le but de l'attaquant est d'écouter ou, plus exactement, d'enregistrer les données brutes sur le réseau local de l'entreprise. Cette attaque utilise le "mode promiscuité" des adaptateurs Ethernet en série qui sont vendus sur le marché. Ce mode permet à un attaquant de saisir chaque paquet circulant sur le réseau. Actuellement, il existe sur le web une multitude de renifleurs de réseau gratuits, qu'un attaquant peut utiliser pour procéder à des écoutes clandestines.

N'importe quel type d'entreprise qui autorise un accès à distance est vulnérable à ce genre d'attaque. Les entreprises ouvertes et les entreprises étendues sont celles pour lesquelles le risque est le plus élevé. La commutation Ethernet est totalement inefficace contre les menaces d'écoute clandestine, étant donné que l'usurpation d'adresse ARP peut complètement corrompre le mécanisme de commutation. Seule une personne procédant à une écoute clandestine de façon peu rigoureuse serait gênée par la commutation Ethernet. Le recours à des techniques de gestion d'accès efficaces et à un chiffrement fort permet de réduire la menace de telles attaques.

Appendice II

Palette des technologies de cybersécurité

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

Les attaques sont de plus en plus sophistiquées et efficaces. Aujourd'hui, les intrus peuvent mettre au point rapidement des attaques exploitant les vulnérabilités découvertes dans les produits. Les attaquants peuvent automatiser ces attaques et les diffuser au grand public. Le Tableau II.1 donne des exemples de la palette des technologies disponibles pour combattre les cybermenaces.

Tableau II.1 – Technologies de cybersécurité

Techniques	Catégorie	Technologie	Objet
Cryptographie	Architecture de certificats et de clés publiques	Signatures numériques	Emettre et tenir à jour des certificats à utiliser dans les communications numériques
		Chiffrement	Chiffrer les données à transmettre ou à stocker
		Echange de clés	Etablir une clé de session ou une clé de transaction à utiliser pour sécuriser une connexion
	Garantie	Chiffrement	Garantir l'authenticité des données
Contrôle d'accès	Protection périmétrique	Pare-feu	Contrôler l'accès à un réseau et depuis un réseau
		Gestion du contenu	Surveiller le trafic afin de détecter des informations non conformes
	Authentification	Facteur unique	Utiliser la combinaison identité d'utilisateur/mot de passe pour vérifier un identificateur
		Double facteur	Utiliser deux éléments pour accorder à un utilisateur l'accès à un système, par exemple la possession d'un jeton physique et la connaissance d'un secret
		Triple facteur	Ajouter un autre facteur d'identification (par exemple biométrie ou mesure d'une caractéristique du corps humain)
		Jetons à puce	Etablir des identificateurs fiables pour les utilisateurs par le biais d'un circuit spécifique dans un dispositif (par exemple une carte à puce)
	Autorisation	Fondée sur le rôle	Contrôler l'accès des utilisateurs à des ressources de systèmes appropriées sur la base du rôle qui leur est assigné
		Fondée sur des règles	Contrôler l'accès des utilisateurs à des ressources de systèmes appropriées sur la base de règles spécifiques associées à chaque utilisateur indépendamment de son rôle dans une organisation

Tableau II.1 – Technologies de cybersécurité

Techniques	Catégorie	Technologie	Objet
Intégrité du système	Antivirus	Méthodes fondées sur la signature	Protéger contre les codes informatiques malveillants (par exemple virus, vers et chevaux de Troie) en utilisant les signatures de ces codes
		Méthodes fondées sur le comportement	Vérifier si les programmes en cours présentent un comportement non autorisé
	Intégrité	Détection des intrusions	Avertir les administrateurs de réseau de la possibilité d'un incident de sécurité (par exemple compromission de fichiers dans un serveur)
Audit et surveillance	Détection	Détection des intrusions	Comparer le trafic dans le réseau et les entrées figurant dans les journaux des hôtes afin de détecter les signatures de données qui indiquent la présence de pirates
	Prévention	Prévention des intrusions	Détecter les attaques dans un réseau et prendre les mesures spécifiées par l'organisation pour réduire les effets des attaques. Les activités suspectes déclenchent des alarmes au niveau des administrateurs et d'autres réponses configurables
	Journalisation	Outils de journalisation	Surveiller et comparer le trafic dans le réseau et les entrées figurant dans les journaux des hôtes afin de détecter les signatures de données et les profils d'adresses d'hôte qui indiquent la présence de pirates
Gestion	Gestion de réseau	Gestion de la configuration	Commander et configurer les réseaux, et gérer les défauts
		Gestion des correctifs	Installer les dernières mises à jour et les derniers programmes de correction dans les dispositifs de réseau
	Politique	Application	Permettre aux administrateurs de procéder à une surveillance et d'appliquer les politiques de sécurité

II.1 Cryptographie

La cryptographie consiste à appliquer des transformations à des données en clair pour les chiffrer en code secret. Le déchiffrement des données secrètes redonne le texte en clair d'origine. Les techniques de cryptographie actuellement disponibles peuvent être utilisées pour chiffrer/déchiffrer les données. Elles peuvent aussi être utilisées pour l'authentification de l'expéditeur d'un message et pour la non-répudiation.

La cryptographie joue un rôle important dans la protection des informations, aussi bien celles qui sont stockées dans un dispositif ou sur un support de stockage que celles qui sont transmises sur une liaison de communication.

En cryptographie, on appelle chiffrement des données la tâche qui consiste à chiffrer les données en code secret au moyen d'algorithmes mathématiques. Quant au déchiffrement des données, il réalise la fonction inverse: appliqué aux données chiffrées, il redonne les données d'origine. La cryptographie utilise des clés secrètes pour réaliser le chiffrement et le déchiffrement.

Les techniques de cryptographie peuvent être classées en deux catégories de base, selon qu'elles sont fondées sur des clés symétriques ou sur des clés asymétriques.

1) La cryptographie à clés symétriques utilise des algorithmes dans lesquels la clé de chiffrement et la clé de déchiffrement sont identiques. La sécurité du modèle dépend de la difficulté à deviner la clé. Les utilisateurs en communication s'entendent sur une clé et ne la divulguent pas aux autres. Les algorithmes à clés symétriques comportent par exemple la norme de chiffrement de données triple (3DES) et la norme de chiffrement perfectionné (AES).

2) La cryptographie à clés asymétriques utilise des algorithmes dans lesquels la clé de chiffrement est différente de la clé de déchiffrement. Dans ce type de cryptographie, l'utilisateur dispose d'une clé privée qui n'est connue que de lui et d'une clé publique qui peut être connue des autres. La clé publique est utilisée par les autres pour chiffrer le texte en clair. Seul le détenteur de la clé privée correspondante pourra déchiffrer le texte chiffré.

Les calculs sont généralement plus rapides dans les techniques de cryptographie à clés symétriques que dans celles à clés asymétriques. Toutefois, la cryptographie à clés symétriques pose un problème essentiel, qui est celui de la distribution des clés, et n'est donc généralement pas adaptée aux déploiements à grande échelle. En revanche, la cryptographie à clés asymétriques (également appelée cryptographie à clé publique) permet de surmonter certaines des limitations de gestion de clé présentées par la cryptographie à clés symétriques. La cryptographie à clé publique est basée sur l'utilisation de certificats numériques pour la gestion et la révocation des clés publiques. Pour accroître la vitesse de calcul, on peut utiliser des techniques de cryptographie à clé publique pour échanger de façon sécurisée une clé symétrique à utiliser dans une session ou dans une transaction.

Les signatures numériques sont un exemple de mise en œuvre pratique de la cryptographie à clé publique. Un certificat numérique garantit l'association entre une clé publique et un détenteur du certificat. Les signatures numériques permettent d'assurer l'authentification, l'intégrité des données et la non-répudiation pour les transactions. Elles peuvent être utilisées pour confirmer l'identificateur déclaré par l'expéditeur d'un message. Elles sont souvent utilisées conjointement avec des certificats numériques. Ceux-ci servent à acheminer les informations nécessaires pour la cryptographie à clé publique et les signatures numériques. Les certificats numériques peuvent être envoyés aux utilisateurs par le biais d'une autorité agréée ou de confiance.

Un code d'authentification de message (MAC) est un total de contrôle d'authentification obtenu par l'application d'un mécanisme d'authentification et d'une clé secrète à un message. Contrairement aux techniques relatives aux signatures numériques, un code MAC est calculé et vérifié au moyen de la même clé. Les codes MAC ne peuvent donc être vérifiés que par le destinataire voulu. Pour les codes MAC fondés sur une fonction de hachage (codes HMAC) (cf. [b-IETF RFC 2104]), une ou plusieurs clés sont utilisées conjointement avec une fonction de hachage pour produire un total de contrôle qui est ajouté au message.

II.2 Techniques de contrôle d'accès

Le contrôle d'accès a pour objet de faire en sorte que seuls les utilisateurs autorisés puissent accéder à un dispositif de réseau ou à un système connecté. En pratique, le contrôle d'accès permet aux professionnels des technologies de l'information de mieux analyser et comprendre le type et la nature des attaques qui se produisent dans leurs réseaux. De nombreuses techniques peuvent être utilisées pour mettre en œuvre le contrôle d'accès. Elles sont examinées dans les paragraphes qui suivent.

II.2.1 Protection périmétrique

La protection périmétrique interdit l'accès à un réseau ou à un ordinateur par des utilisateurs extérieurs non fiables ou non autorisés. Pour cela, une frontière logique ou physique est installée entre les zones protégées et les zones ouvertes au public et aux utilisateurs externes non fiables (non compris les utilisateurs internes non fiables). La protection périmétrique peut être utilisée pour

protéger un réseau ou un seul dispositif. Les technologies employées sont par exemple les suivantes:

1) Les logiciels de filtrage du contenu ou de gestion du contenu limitent le type de données auxquelles il est possible d'accéder ou qui peuvent être distribuées dans un réseau (cf. [b-ISO/CEI 10828-3]). Ils limitent la possibilité pour les utilisateurs d'accéder à un contenu en dehors de leur frontière, ce qui minimalise les risques de télécharger des virus ou d'autres codes malveillants provenant d'endroits non fiables. Le filtrage de contenu peut prendre la forme d'un filtrage d'adresses URI (cf. [IETF RFC 2396]), qui refuse l'accès des utilisateurs à des pages web dont le contenu est douteux. Le filtrage de contenu peut être utilisé pour analyser les messages d'application (messages électroniques par exemple) afin de détecter les spams, virus et contenus non approuvés.

2) Pare-feu: les pare-feu (cf. [b-ISO/CEI 10828-3]) peuvent être classés en quatre grandes catégories: filtres de paquets, passerelles au niveau des circuits, passerelles au niveau des applications et pare-feu d'inspection multicouches à états.

   - Les pare-feu à filtrage de paquets fonctionnent au niveau de la couche IP. Ils font généralement partie d'un pare-feu routeur. Ils comparent chaque paquet IP à un ensemble défini de règles avant que ce paquet soit transmis à la route suivante ou à sa destination finale. Suivant les résultats de la comparaison, le pare-feu élimine le paquet, le retransmet ou envoie un message à l'expéditeur. Les règles peuvent porter sur l'adresse IP d'origine et l'adresse IP de destination, le numéro de port d'origine et le numéro de port de destination ainsi que le protocole utilisé. Les routeurs avec traduction d'adresse réseau (NAT) présentent les avantages des pare-feu à filtrage de paquets et permettent en outre de masquer les adresses IP des dispositifs situés derrière le pare-feu. Les pare-feu à filtrage de paquets ont une faible incidence sur la qualité de fonctionnement du réseau et offrent une certaine sécurité au niveau de la couche réseau.
   - Les passerelles au niveau des circuits fonctionnent au niveau de la couche TCP des protocoles TCP/IP pour surveiller les messages de prise de contact TCP parmi les paquets et ce afin de déterminer si une session demandée est légitime ou non. En outre, les demandes adressées à un ordinateur distant par le biais d'une passerelle au niveau des circuits apparaîtront au niveau du récepteur comme si elles provenaient de la passerelle. Cette technique facilite le masquage des informations concernant un réseau protégé. Les passerelles au niveau des circuits ne filtrent pas les paquets individuels.
   - Les proxys ou les passerelles au niveau des applications filtrent les paquets au niveau de la couche application du modèle OSI. Les demandes entrantes ou sortantes d'accès à des services sans proxy sont refusées. Les proxys examinent les paquets au niveau de la couche application pour filtrer les commandes propres à l'application telles que HTTP POST (cf. [b-IETF RFC 2616]). Un proxy empêchera le trafic non configuré d'atteindre l'application. Des proxys peuvent aussi être utilisés pour journaliser les activités et les connexions des utilisateurs. Ils offrent un niveau élevé de sécurité, au prix d'une incidence considérable sur la qualité de fonctionnement du réseau.
   - Les pare-feu d'inspection multicouches à états combinent les aspects des types de pare-feu susmentionnés. Les pare-feu multicouches filtrent les paquets au niveau de la couche réseau, établissent si les paquets de session sont valables et filtrent le contenu des paquets au niveau de la couche application. Ils sont transparents du point de vue des connexions entre l'émetteur et le récepteur.

3) Traduction d'adresse réseau (NAT): cette technologie permet de masquer le plan d'adressage de réseau utilisé derrière l'environnement d'un pare-feu. La traduction NAT transpose l'adresse IP d'un système dans le réseau interne en une adresse IP routable externe correspondante différente. Elle permet à de nombreux systèmes situés derrière un pare-feu de partager la même adresse IP externe. Les ressources situées derrière un pare-feu restent accessibles par les utilisateurs externes grâce à la transmission des connexions entrantes sur certains numéros de port. La traduction NAT peut être mise en œuvre sur la plupart des dispositifs de réseau tels que les commutateurs, les routeurs et les pare-feu.

4) Passerelles au niveau des applications: ces systèmes (cf. [b-ISO/CEI 10828-3]) comportent un dispositif ou un ensemble de dispositifs de type matériel ou logiciel. Ils sont conçus pour restreindre l'accès entre deux réseaux distincts et, pour cela, ils utilisent des techniques de proxy d'application et d'inspection de paquets à états. Des combinaisons et des variantes (par exemple pare-feu au niveau des circuits) de ces techniques peuvent aussi être utilisées. En outre, la traduction NAT peut être effectuée par les passerelles au niveau des applications.

5) Proxy d'application: ces systèmes (cf. [b-ISO/CEI 10828-3]) permettent de connaître les tentatives de connexion au niveau des applications en examinant les paquets au niveau de la couche la plus élevée de la pile de protocoles. Les proxys d'application ont une visibilité complète des échanges de données au niveau de la couche application, ce qui leur permet de voir facilement et directement les menus détails de chaque tentative de connexion et d'appliquer ensuite des politiques de sécurité. Les proxys d'application peuvent être dotés de la capacité de mettre fin à des connexions de client et d'établir une nouvelle connexion vers un réseau protégé interne. Cette capacité permet d'améliorer la sécurité du fait de la séparation des systèmes externes et internes.

II.2.2 Réseau privé virtuel (VPN)

Le document [b-ISO/CEI 18028-5] présente de façon détaillée l'utilisation de VPN pour sécuriser les communications dans les réseaux.

Les VPN sont actuellement utilisés pour interconnecter des réseaux ainsi que pour raccorder des utilisateurs distants à des réseaux. Dans leur forme la plus simple, ils comportent un mécanisme permettant d'établir un ou plusieurs canaux de données sécurisés sur une connexion point à point ou un réseau existant. Ils peuvent être établis et supprimés dynamiquement. Le réseau hôte peut être privé ou public.

L'accès à distance au moyen d'un VPN est mis en œuvre sur une connexion point à point normale qui est déjà établie entre l'utilisateur local et l'emplacement distant (cf. [b-ISO/CEI 18028-5]). Les VPN peuvent être assurés sous la forme d'un service géré dans lequel une connectivité, une gestion et un adressage sécurisés et fiables, équivalents à ceux qui sont pris en charge dans un réseau privé, sont assurés sur une infrastructure partagée.

Il existe plusieurs représentations possibles des types de VPN (cf. [b-ISO/CEI 18028-5]). En principe, un VPN peut être:

– une connexion point à point unique (par exemple un dispositif de client accédant à distance au réseau d'une entreprise par le biais d'une passerelle de site); ou

– une connexion point à nuage (utilisation de techniques MPLS).

Il existe trois principaux types de VPN (cf. [b-ISO/CEI 18028-5]):

– Les VPN de couche 2 émulent une fonctionnalité de réseau local et, pour cela, utilisent des connexions VPN fondées sur un réseau hôte pour relier les sites d'une entreprise ou pour offrir une connexion à distance à une organisation. Les offres des fournisseurs incluent généralement un service de liaison privée virtuelle (VPWS), qui fournit une connexion fondée uniquement sur des liaisons simulées, ou un service de réseau local privé virtuel (VPLS), qui fournit un service de réseau local émulé plus complet.

– Les VPN de couche 3 émulent une fonctionnalité de réseau étendu et, pour cela, utilisent des VPN fondés sur une infrastructure de réseau. Ils offrent la possibilité d'utiliser des plans d'adressage IP privés sur une infrastructure publique, une pratique qui ne serait pas autorisée sur des connexions IP publiques. Toutefois, l'utilisation d'adresses privées dans des réseaux publics via des dispositifs NAT peut compliquer l'établissement et l'utilisation de VPN IPSec (cf. [b-IETF RFC 2411]).

– Les VPN de couche 4 sont utilisés pour sécuriser les transactions dans les réseaux publics. Dans ce type de VPN, les connexions sont généralement établies sur TCP, qui est un protocole de couche 4. Les VPN de ce type offrent un canal sécurisé entre les applications en communication afin de garantir la confidentialité et l'intégrité des données pendant la durée de la transaction.

Des VPN peuvent être mis en œuvre dans un réseau privé sous le contrôle de l'entreprise détentrice ou ils peuvent être mis en œuvre entre des réseaux dans le domaine public. Les mises en œuvre fondées sur des combinaisons de ces deux schémas sont également possibles. Par ailleurs, on peut établir des canaux sécurisés en utilisant des tunnels passant dans les réseaux des fournisseurs d'accès à l'Internet. A cet égard, l'Internet public est, de fait, le système de transport sous-jacent et, en tant que tel, les risques d'atteinte à la confidentialité des données acheminées par le VPN sont plus élevés.

Un tunnel est un trajet de données entre des dispositifs raccordés à un réseau, qui est établi sur une infrastructure de réseau existante. Le tunnel est transparent pour le fonctionnement du réseau. Un VPN créé avec des tunnels est généralement plus souple qu'un réseau fondé sur des liaisons physiques. Des tunnels peuvent être créés au moyen de circuits virtuels, d'une commutation par étiquette ou d'une encapsulation de protocole.

Les aspects de sécurité des divers types de VPN sont présentés dans le Tableau II.2.2 (cf. [b-ISO/CEI 18028-5]).

Tableau II.2.2 – Aspects de sécurité des VPN

VPN	Technologie	Authentification d'utilisateur	Chiffrement des données	Gestion de clé	Contrôle d'intégrité
VPN de couche 2	Relais de trame, ATM, MPLS, PPP, L2F	N/A	N/A	N/A	N/A
	L2TP (cf. [b-IETF RFC 2661])	De type CHAP	N/A	N/A	N/A

Tableau II.2.2 – Aspects de sécurité des VPN

VPN	Technologie	Authentification d'utilisateur	Chiffrement des données	Gestion de clé	Contrôle d'intégrité
VPN de couche 3	IPSec	Clés secrètes prépartagées fondées sur des certificats (paquet)	Plusieurs algorithmes négociables (paquet)	IKE	Négociable
	IPSec avec L2TP	Clés secrètes prépartagées fondées sur des certificats (paquet)	Plusieurs algorithmes négociables (paquet)	IKE	Négociable
VPN de couche 4	MPLS	N/A	N/A	N/A	N/A
	TLS	Fondée sur des certificats	Négociable	Négociable	Négociable
	Connecteur sécurisé	Paire de clés générée par le système (pas de certificat)	Négociable	Transfert de clés publiques à l'expéditeur de données	Négociable
NOTE 1 – On peut utiliser le protocole SSL au lieu du protocole TLS. NOTE 2 – Le document [b-IETF RFC 3031] donne un aperçu de l'architecture de commutation par étiquette multiprotocole (MPLS). Le document [b-IETF RFC 1661] décrit le protocole point à point (PPP). Le document [b-IETF RFC 2427] traite de l'interconnexion multiprotocole sur relais de trame.					

II.2.3 Authentification

Pour authentifier un utilisateur, on peut utiliser plusieurs méthodes, par exemple fondées sur des mots de passe, sur des mots de passe à usage unique, sur des techniques biométriques, sur des cartes à puce [b-ISO/CEI 7816-x] ou sur des certificats. L'authentification par mot de passe doit utiliser des mots de passe forts (comportant par exemple au moins huit caractères, avec au moins un caractère alphabétique, un caractère numérique et un caractère spécial). L'authentification par mot de passe seule peut être insuffisante. Sur la base d'une évaluation des vulnérabilités, il peut être nécessaire de combiner l'authentification par mot de passe avec d'autres méthodes d'authentification et d'autorisation, par exemple fondées sur des certificats, le protocole simple d'accès à l'annuaire (LDAP) (cf. [b-IETF RFC 3377]), le service d'authentification à distance des utilisateurs entrants (RADIUS) (cf. [b-IETF RFC 2869], [b-IETF RFC 3579] et [b-IETF RFC 3580]), le protocole Kerberos (cf. [b-IETF RFC 1510]) et l'infrastructure de clé publique (PKI) (cf. [b-IETF RFC 2459]).

Les systèmes d'authentification peuvent être classés suivant le nombre de facteurs d'identification nécessaires. L'authentification à un seul facteur désigne un système qui utilise un seul facteur (par exemple une combinaison identité d'utilisateur/mot de passe). L'authentification à deux facteurs correspond à un système qui nécessite deux éléments pour pouvoir obtenir un accès (par exemple la possession d'un jeton physique plus la connaissance d'un secret (par exemple mot de passe)). Un système à trois facteurs comporte un autre facteur d'identification (par exemple biométrie ou mesure d'une caractéristique du corps humain). Si l'on emploie davantage de facteurs, l'authentification sera plus sûre; toutefois, plus on inclut de facteurs, plus on augmente la complexité, le coût et la charge de gestion. Dans un système d'authentification donné, la principale difficulté est de trouver le compromis optimal entre simplicité et sécurité.

L'authentification à un seul facteur correspondant à la combinaison identité d'utilisateur/mot de passe est actuellement le plus couramment utilisée. Les systèmes d'authentification par mot de passe sont simples, faciles à gérer et très conviviaux. Si on utilise des mots de passe forts, l'authentification à un seul facteur offre un niveau élevé de sécurité. Toutefois, les systèmes existants fondés sur des mots de passe ont posé quelques difficultés car il est très difficile pour les utilisateurs de retenir plusieurs mots de passe forts. Comme cela sera abordé dans les recommandations ci-dessous, ces inconvénients peuvent être réduits au minimum dans le cadre d'une solution optimale correspondant à un système "à un seul mot de passe fort".

Des jetons (par exemple des cartes à puce) sont ajoutés comme deuxième facteur dans bon nombre de systèmes d'authentification. Ils offrent une sécurité d'authentification supplémentaire étant donné que l'utilisateur doit prouver qu'il possède physiquement le jeton pour pouvoir être authentifié. Un attaquant devrait aussi posséder le jeton de l'utilisateur pour pouvoir obtenir un accès. Toutefois, le niveau plus élevé d'authentification entraîne des coûts supplémentaires liés aux jetons et lecteurs de jetons nécessaires. En outre, les jetons peuvent facilement se perdre, auquel cas il faut les réémettre, ce qui peut entraîner une surcharge de gestion élevée.

Une authentification forte fondée sur la cryptographie peut être assurée sur la base de certificats numériques envoyés aux utilisateurs et stockés sur des jetons ou dans la mémoire de l'ordinateur de l'utilisateur. Des algorithmes cryptographiques sont utilisés pour garantir qu'un certificat donné a bien été envoyé de façon légitime à un utilisateur. On utilise une infrastructure de clé publique pour l'envoi et la tenue à jour des certificats numériques. Les systèmes d'authentification forte fondée sur la cryptographie assurent une authentification très forte mais ils sont onéreux et entraînent une surcharge de gestion, et ne sont donc actuellement adoptés que dans des environnements hautement sécurisés.

II.2.4 Autorisation

Une fois l'authentification réalisée, des mécanismes d'autorisation contrôlent l'accès de l'utilisateur aux ressources de système appropriées. Ils peuvent être classés suivant la granularité du contrôle, c'est-à-dire suivant le nombre de subdivisions entre les ressources de système. Une autorisation à granularité fine se rapporte de façon générique à un système pour lequel le contrôle d'accès se fait par très petites tranches (par exemple au niveau de chaque application ou service).

L'autorisation est souvent "fondée sur le rôle", auquel cas l'accès aux ressources de système est fondé sur le rôle assigné à une personne dans une organisation. Le rôle d'administrateur de système peut avoir un accès hautement privilégié à toutes les ressources de système tandis que le rôle d'utilisateur général n'a normalement accès qu'à un sous-ensemble de ces ressources. Si une autorisation à granularité plus fine est appliquée, le rôle d'administrateur des ressources humaines peut avoir un accès exclusif aux bases de données des ressources humaines hautement confidentielles et le rôle de comptable peut avoir un accès exclusif aux bases de données du système de comptabilité.

L'autorisation peut aussi être "fondée sur des règles", auquel cas l'accès aux ressources de système est fondé sur des règles spécifiques associées à chaque utilisateur indépendamment de son rôle dans une organisation. Par exemple, des règles peuvent être mises en place pour autoriser un accès en lecture seule ou un accès en lecture/écriture à la totalité ou à une partie des fichiers contenus dans un système.

II.2.5 Protocoles d'authentification et d'autorisation

D'une manière générale, plusieurs protocoles ont été adoptés pour les services d'authentification. Le protocole RADIUS (service d'authentification à distance des utilisateurs entrants) (cf. [b-IETF RFC 2865]) est largement utilisé pour centraliser les services d'authentification par mot de passe. Conçu au départ pour l'authentification des utilisateurs entrants à distance, le protocole RADIUS a été adopté pour les services d'authentification générale des utilisateurs. Le protocole LDAP (protocole simple d'accès à l'annuaire) est largement utilisé dans les systèmes

d'authentification et d'autorisation. Il permet un stockage aisé des justificatifs d'identité des utilisateurs pour leur authentification et leur autorisation.

Les serveurs d'authentification RADIUS sont souvent couplés à un stockage des justificatifs d'identité dans des annuaires LDAP afin de disposer d'un système centralisé pour l'authentification et l'autorisation. Normalement, lorsqu'un utilisateur tente d'accéder à une application particulière sur ce type de système, l'application demande les justificatifs d'identité de l'utilisateur pour son authentification puis transmet ces justificatifs au système centralisé. Le serveur RADIUS compare alors les justificatifs présentés à ceux stockés dans la base de données LDAP et consulte par ailleurs les informations relatives aux règles d'autorisation contenues dans la base de données LDAP. Le résultat de l'authentification (réussite ou échec) est retourné à l'application conjointement avec les informations relatives aux règles d'autorisation concernant l'utilisateur en question. Les règles d'autorisation sont alors appliquées au niveau de l'application pour permettre à l'utilisateur d'accéder à des données ou à des services particuliers. Du point de vue de l'utilisateur final, ces systèmes d'authentification et d'autorisation devraient être automatiques et faciles à utiliser.

II.3 Antivirus et intégrité du système

Des vers, des codes malveillants, des virus et des chevaux de Troie peuvent modifier un système et ses données. Il est donc essentiel d'utiliser des technologies permettant de détecter les virus et de garantir le maintien de l'intégrité du système.

Un ver est un programme qui s'autoreproduit et passe d'un système à un autre sans qu'une intervention humaine ne soit nécessaire. Un virus peut se rattacher à des fichiers d'utilisateur et peut soudainement devenir actif en s'autoreproduisant dans d'autres fichiers lorsqu'un utilisateur peu méfiant exécute une certaine action, par exemple ouvre un fichier infecté. Quant au cheval de Troie, il apparaît généralement à l'utilisateur peu méfiant comme un programme utile alors qu'il s'agit d'un programme dans lequel est caché un code nuisible.

La technologie antivirus permet de protéger les systèmes contre les attaques par des vers, par des codes malveillants ou par des chevaux de Troie. Les logiciels antivirus peuvent soit être installés sur les dispositifs des utilisateurs soit être fournis sous la forme d'un service assuré par le réseau ou par le fournisseur d'accès à l'Internet. Les techniques relatives à l'intégrité du système reposent sur des logiciels qui vérifient que seules les mises à jour autorisées sont appliquées aux fichiers essentiels du système.

Les produits logiciels antivirus peuvent utiliser des techniques fondées sur des signatures de type chaîne pour identifier les virus et les codes malveillants. Ce type de technique nécessite de connaître au préalable les codes malveillants pour que le logiciel antivirus puisse les détecter. La base de données des signatures doit donc être à jour pour pouvoir assurer une protection efficace.

Les analyseurs d'activité recherchent les activités non autorisées réalisées par un code en fonctionnement et informent l'utilisateur des activités suspectes. Ils ont généralement une efficacité limitée contre les virus mais peuvent être plus efficaces contre les vers et les chevaux de Troie. Les analyseurs heuristiques statiques analysent le code pour essayer de déterminer les activités qui pourraient être associées à un comportement de type virus.

Les techniques relatives à l'intégrité du système reposent sur des logiciels qui contrôlent les modifications apportées aux fichiers essentiels du système. Les administrateurs informatiques peuvent les utiliser pour contrôler le système afin de déterminer si des pirates ont réussi à pénétrer dans un système (les pirates ont tendance à laisser des portes dérobées).

II.4 Audit et surveillance

Les techniques d'audit et de surveillance permettent aux administrateurs informatiques d'évaluer la sécurité globale d'un système, y compris les logiciels de détection et de prévention des intrusions. Les administrateurs informatiques peuvent utiliser ces techniques pour analyser le système afin de

déterminer ses faiblesses après une attaque. Dans certains cas, une analyse du système peut être réalisée pendant qu'une attaque active frappe le système.

Un système de détection des intrusions (IDS) (cf. [b-ISO/CEI 18043]) peut être utilisé pour surveiller le réseau afin de faire en sorte qu'aucun utilisateur non autorisé n'accède au réseau. La plupart des applications IDS comparent le trafic dans le réseau et les entrées figurant dans les journaux des hôtes afin de détecter les signatures de données et les profils d'adresses d'hôte qui indiquent la présence de pirates. Le logiciel de détection des intrusions identifie les séquences de trafic qui indiquent la présence d'utilisateurs non autorisés. Les activités suspectes déclenchent des alarmes au niveau des administrateurs et d'autres réponses configurables. On définit plusieurs grandes catégories de systèmes de détection des intrusions (IDS) en fonction des critères suivants:

- délai de détection des incidents: en temps réel ou en différé, suivant si les journaux de système et le trafic de réseau sont analysés au fur et à mesure que les événements se produisent ou s'ils sont analysés par lots en dehors des heures de fonctionnement;
- type d'installation: sur le réseau ou sur des hôtes. Un système IDS sur le réseau fait généralement intervenir plusieurs moniteurs (ce sont souvent des dispositifs préconfigurés) installés aux points de passage obligés dans le réseau (là où l'ensemble du trafic entre deux points peut être surveillé). Un système IDS sur des hôtes nécessite que le logiciel soit installé directement sur les serveurs à protéger et qu'il surveille les connexions au réseau et les activités des utilisateurs sur ces serveurs; et
- type de réaction aux incidents: soit le système IDS intervient activement pour déjouer les attaques (par exemple en modifiant les règles applicables aux pare-feu ou les filtres des routeurs) soit il ne fait que transmettre le problème au personnel ou à d'autres systèmes de réseau.

La plupart des produits IDS commerciaux comportent à la fois des capacités de surveillance fondées sur le réseau et des capacités de surveillance fondés sur des hôtes, un hôte de gestion central étant chargé de recevoir les rapports issus des divers moniteurs et d'alerter le personnel responsable de la supervision du réseau. L'utilisation d'un produit IDS fondé sur le réseau est recommandée pour la plupart des installations de réseau en fonction des besoins particuliers des clients.

II.5 Gestion

Les techniques de gestion de la configuration permettent aux administrateurs informatiques de fixer et de vérifier les paramètres de sécurité des dispositifs de leurs réseaux. La gestion de politique permet aux administrateurs informatiques de définir des politiques de sécurité et de qualité de service axées sur les activités et de les appliquer dans toute l'organisation sans qu'il soit nécessaire de comprendre l'ensemble des règles et des paramètres propres aux dispositifs qui sont amenés à appliquer ces politiques. Sur le plan technique, ces politiques sont un ensemble de règles régissant l'administration et la gestion des ressources informatiques ainsi que le contrôle d'accès à ces ressources; elles doivent être établies sur la base des orientations commerciales définies par l'organisation. Sur le plan de la sécurité, la gestion de politique permet de faire face à la complexité et aux courbes d'apprentissage difficile associées aux technologies telles que les pare-feu, les systèmes IDS, les listes et filtres d'accès et les techniques d'authentification ainsi qu'à l'insuffisance de visibilité du système sur les différentes parties du réseau (centre de données, bureaux distants, campus).

Les solutions permettant de résoudre certaines parties du problème sont nombreuses, mais le système de gestion de politique idéal offre une configuration de réseau centralisée, garantissant que les paramètres de sécurité sont fixés de façon cohérente entre les différents nœuds, afin de réduire le risque de vulnérabilité du réseau. Cela ne signifie pas qu'il existe un seul système de politique; dans les réseaux plus vastes comportant plusieurs domaines administratifs, il peut être nécessaire d'avoir plusieurs systèmes de politique, chacun étant chargé de contrôler un sous-ensemble des dispositifs et de contribuer à la cohérence interdomaines.

Un système de gestion de politique entièrement mis en œuvre a pour principal avantage d'être facile à utiliser et d'offrir un environnement plus sûr. Idéalement, les gestionnaires de réseau aimeraient pouvoir définir des politiques d'exploitation de réseau en utilisant un vocabulaire non technique, ces politiques étant ensuite traduites automatiquement par le système de politique en mécanismes de sécurité appropriés à mettre en œuvre dans le réseau.

II.5.1 Modèle de référence de la gestion de politique

La Figure II.5.1 présente le cadre architectural de l'IETF applicable à la gestion de politique ([b-IETF RFC 2753]). Ce cadre sert de modèle de référence pour la gestion de politique, à la fois en termes de sécurité et de qualité de service. Lorsque la gestion de politique est fondée sur ce modèle, elle sera donc mise en œuvre dans tout le réseau et dans toutes les couches de l'architecture et sera mise à la disposition de tous les types d'utilisateurs et d'applications, y compris les employés, les techniciens réseau, les partenaires et même les clients.

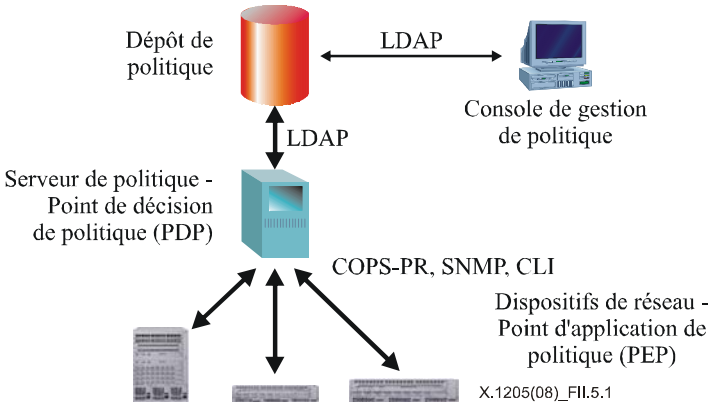

Figure II.5.1 – Modèle de référence de la gestion de politique

Les éléments de ce modèle sont les suivants:

- *Point d'application de politique (PEP)*: il s'agit d'un dispositif de réseau ou de sécurité qui accepte une politique (règles de configuration) provenant du point de décision de politique et qui applique cette politique au trafic de réseau le traversant, sur la base des mécanismes de réseau et des mécanismes de sécurité fondés sur le réseau appropriés.
- *Point de décision de politique (PDP)*: les points PDP ou serveurs de politique transposent les politiques de réseau en messages spécifiques de commande de dispositif, qui sont ensuite transmis aux points d'application de politique. Ces serveurs de politique sont souvent des systèmes autonomes qui commandent la totalité des commutateurs et des routeurs situés dans un domaine administratif particulier; ils communiquent avec ces dispositifs au moyen d'un protocole de commande (par exemple COPS, commandes Set SNMP, Telnet ou interface de ligne de commande (CLI) propre à un dispositif).
- *Service commun de politique ouverte (COPS)*: le protocole COPS est un protocole simple de demande et réponse à états fondé sur TCP qui peut être utilisé pour échanger des informations de politique entre un point de décision de politique (PDP) et ses points d'application de politique clients (PEP). Il est spécifié dans le document [b-IETF RFC 2748]. Dans le cadre du protocole COPS, les points PEP doivent établir des connexions permanentes avec un point PDP primaire (et un point PDP secondaire lorsque le point PDP primaire est inaccessible). Une autre solution consiste à utiliser un dispositif proxy COPS, qui traduit les messages COPS provenant d'un serveur de politique en commandes SNMP ou CLI comprises par les dispositifs de réseau et de sécurité.

Le protocole COPS prend en charge deux modèles d'extension différents pour le contrôle de politique, un modèle de sous-traitance dynamique COPS-RSVP, spécifié dans le document [b-IETF RFC 2749], et un modèle de configuration ou d'approvisionnement COPS-PR, spécifié dans le document [b-IETF RFC 3084]. Les extensions d'approvisionnement du protocole COPS permettent au point PDP d'installer à l'avance des politiques au niveau des points PEP, ce qui permet à ces derniers de prendre des décisions de politique pour les paquets de données sur la base de ces informations préapprovisionnées. La communication doit être poursuivie entre les points PDP et PEP pour que les politiques approvisionnées dans le dépôt de données (à savoir l'annuaire) restent synchronisées avec celles qui sont envoyées aux points PEP.

- *Dépôt de politique*: l'annuaire du réseau rassemble toutes les informations de politique; il décrit les utilisateurs, les applications, les ordinateurs et les services du réseau (c'est-à-dire les objets et les attributs) ainsi que les relations entre ces entités. L'adresse IP et l'utilisateur final font l'objet d'une intégration étroite (par le biais du protocole de configuration d'hôte dynamique – DHCP et d'un système de noms de domaine – DNS). Un annuaire est généralement mis en œuvre sur une machine spécialisée fondée sur une base de données. Le protocole simple d'accès à l'annuaire est le mécanisme utilisé par les serveurs de politique pour accéder à l'annuaire.

  Le dépôt de politique est utilisé pour stocker des informations relativement statiques concernant le réseau (par exemple configurations de dispositif), tandis que les serveurs de politique stockent des informations d'état de réseau plus dynamiques (par exemple attribution de largeur de bande ou informations concernant les connexions établies). Un serveur de politique extrait les informations de politique de l'annuaire et les applique dans les éléments de réseau appropriés.

  Aucune norme en vigueur ne décrit la structure de la base de données de l'annuaire, c'est-à-dire la manière dont les objets de réseau et leurs attributs sont définis et représentés. Un schéma d'annuaire commun est nécessaire si on veut que les applications de plusieurs fournisseurs puissent partager les mêmes informations d'annuaire; par exemple, tous les fournisseurs ont besoin d'un axe commun pour interpréter et stocker des informations de configuration concernant les routeurs. La norme DEN à venir (*directory-enabled networking*), actuellement élaborée par le DMTF (*desktop management task force*), vise à répondre à ce besoin. La norme DEN définit un modèle d'information représentant de façon abstraite les profils et les politiques, les dispositifs, les protocoles et les services. Elle décrit un modèle unifié permettant d'intégrer les utilisateurs, les applications et les services de réseau, et un cadre extensible orienté vers les services.

- *Protocole simple d'accès à l'annuaire* (LDAP version 3): spécifié dans le document [b-IETF RFC 3377], le protocole LDAP est un protocole client-serveur permettant d'accéder à un service d'annuaire. Le modèle d'informations du protocole LDAP est fondé sur l'entrée, qui contient des informations sur un objet donné (par exemple une personne) et qui est composé d'attributs, lesquels ont un type et une ou plusieurs valeurs. Chaque attribut a une syntaxe qui détermine les sortes de valeurs qui sont autorisées dans l'attribut et le comportement de ces valeurs pendant le fonctionnement de l'annuaire.

- *Console de gestion de politique*: les êtres humains interagissent avec le système de gestion de politique par le biais d'une console de gestion, généralement installée sur un ordinateur personnel ou sur une station de travail. Une autre solution consiste à utiliser un navigateur web pour permettre aux gestionnaires d'accéder de pratiquement n'importe où, une sécurité au niveau des objets de politique étant mise en place pour limiter les politiques qui peuvent être modifiées par un individu donné. C'est par le biais de la console de gestion que les politiques sont instanciées dans l'annuaire. La console comporte une interface utilisateur graphique et les outils dont les gestionnaires ont besoin pour définir les politiques de réseau en tant que règles régissant les activités. Elle peut aussi permettre à l'opérateur d'accéder à

des configurations de sécurité de niveau inférieur dans les différents commutateurs et routeurs.

Les éléments du modèle de référence de la gestion de politique interagissent pour assurer une gestion de politique en boucle fermée et notamment pour configurer les dispositifs périphériques, pour appliquer les politiques dans le réseau et pour vérifier la fonctionnalité du réseau telle qu'elle est vue par l'application de l'utilisateur final. L'application des politiques dans le réseau comporte les contrôles d'admission des applications ou des utilisateurs souhaitant accéder à des ressources du réseau. La gestion de politique peut contribuer à simplifier l'environnement de gestion de la configuration à l'intérieur des entreprises, ce qui permet de réduire au minimum les risques d'erreur humaine.

II.5.2 Renforcement du système d'exploitation des serveurs

Le renforcement du système d'exploitation (OS) est un élément essentiel de la sécurisation des systèmes d'information dans la couche de sécurité relative aux applications. Une entreprise dispose généralement de plusieurs systèmes d'exploitation différents pour diverses applications de données (y compris la gestion de réseau), mais aussi pour les serveurs d'application prenant en charge la téléphonie IP et des applications où les communications sont nombreuses. Il est relativement fréquent que plusieurs versions du même type de système d'exploitation soient déployées dans l'infrastructure des technologies de l'information, ce qui rend encore plus difficiles les tâches liées à la sécurité.

Le système d'exploitation le plus courant dans le monde des données est également largement utilisé pour les serveurs d'application prenant en charge la téléphonie IP et des applications où les communications sont nombreuses. Les fournisseurs offrent une version renforcée des systèmes d'exploitation avec des logiciels de sécurité de série pour des fonctions comme la protection antivirus, la détection des intrusions et les audits de connexion. Pour renforcer un système d'exploitation, il faut d'abord éviter le clonage de serveur et fiabiliser les supports à partir desquels le système d'exploitation est téléchargé. Pour les systèmes d'exploitation pour lesquels il n'existe pas de guide spécifique de renforcement, il convient de consulter le fournisseur de ces systèmes pour obtenir les dernières procédures et les derniers correctifs pour le renforcement.

Appendice III

Exemples de sécurité dans les réseaux

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

Le présent appendice donne des exemples de sécurisation de divers aspects d'une organisation ou d'une grande entreprise au moyen des techniques exposées dans la présente Recommandation.

En particulier, l'élaboration de solutions de sécurité par couches pour sécuriser un campus repose sur des passerelles vers l'Internet, un centre de données, des bureaux distants, l'accès à distance et la téléphonie IP. On utilise les techniques exposées dans la présente Recommandation pour montrer que la sécurité pour l'entreprise ne correspond pas à un modèle à taille unique. Le Tableau III.1 donne des exemples des aspects de sécurité à prendre en considération. L'exemple N° 1 correspond à une entreprise de petite taille qui utilise des lignes privées physiques limitées entre ses sites et qui fournit un accès à distance limité à ses employés, la présence sur le web étant assurée par le biais d'un centre de données Internet géré par un fournisseur de services (qui est chargé d'établir un environnement sécurisé). L'exemple N° 2 correspond à une entreprise ouverte avec un modèle de fonctionnement fondé sur l'Internet, qui permet aux partenaires, fournisseurs et clients d'avoir un accès limité aux applications gérées par l'entreprise. Dans cet exemple, les utilisateurs internes et les utilisateurs externes accèdent au réseau de l'entreprise depuis leur domicile, des bureaux distants ou d'autres réseaux, en utilisant des dispositifs filaires ou mobiles.

Tableau III.1 – Aspects de sécurité pour différents types d'entreprise

Domaine de réseau	Exemple d'entreprise N° 1	Exemple d'entreprise N° 2
Sécurisation du campus	Oui	Oui, représentant des exigences de sécurité plus strictes
Sécurisation des bureaux distants	Option de chiffrement sur les lignes privées physiques ou virtuelles	Oui, y compris l'accès à l'Internet depuis les bureaux distants
Sécurisation de l'accès à distance	Oui, mais uniquement pour l'accès commuté privé	Oui, y compris les partenaires et les clients
Sécurisation du centre de données	Oui pour les centres de données internes	Oui, y compris les centres de données Internet
Sécurisation de la téléphonie IP	Oui	Oui, utilisation de VPN

III.1 Sécurisation de l'accès à distance

Les technologies d'accès à distance permettent à une entreprise ou à une organisation d'utiliser efficacement les personnes et les ressources situées pratiquement n'importe où. Toutefois, elles sont aussi susceptibles de poser des problèmes de sécurité à l'entreprise. Les employés de l'entreprise qui sont en déplacement ou qui travaillent depuis leur domicile constituent la majorité des utilisateurs de l'accès à distance, mais cette catégorie inclut également les petits bureaux, qui se raccordent sur demande au réseau de l'entreprise. Les principaux problèmes sont résolus grâce à la sécurité dans le réseau et à une gestion d'accès sécurisée. La sécurité de gestion du réseau est mise en œuvre au niveau du site central. La sécurité des applications est importante dans le sens où le dispositif distant a besoin d'être protégé au moyen de logiciels antivirus et de pare-feu personnels.

Une menace importante qui vise spécifiquement les utilisateurs distants est le vol de leur équipement. Le vol de l'équipement d'un utilisateur distant ne devrait pas permettre d'intrusion dans

d'autres domaines du réseau de l'entreprise ni d'accès aux informations qui peuvent être stockées dans le système. Toutefois, les utilisateurs mobiles souhaitent pouvoir transporter leurs dispositifs ou terminaux pour pouvoir accéder au réseau partout. Il est donc nécessaire de chiffrer les informations sensibles stockées sur des systèmes utilisés pour l'accès à distance, de préférence au moyen d'un système qui s'intègre de façon transparente dans l'utilisation normale des applications. Les systèmes de chiffrement actuellement disponibles permettent un fonctionnement normal du point de vue de l'utilisateur, aucun chiffrement/déchiffrement manuel ou individuel des fichiers n'étant requis. Par exemple, des systèmes de fichiers entiers ou "dossiers" peuvent être stockés sous forme chiffrée, le déchiffrement étant intégré dans l'accès normal à ces systèmes. Une autre forme de menace peut surgir lorsque l'utilisateur distant utilise un réseau local sans fil, éventuellement à son domicile ou dans un hôtel. Dans ce cas, Il est important de disposer d'un antivirus et d'un pare-feu personnel à jour.

Les formes les plus courantes d'accès à distance pour les communications de données sont l'accès commuté, soit directement à l'entreprise soit à un fournisseur d'accès à l'Internet, et l'accès direct fondé sur l'Internet au moyen d'une ligne d'abonné numérique (DSL), de câblo-modems, de l'Ethernet natif (par exemple dans des hôtels) et de réseaux locaux sans fil (par exemple dans des aéroports). Les services publics de transmission de données sans fil prenant en charge l'accès à l'Internet constituent également un domaine à forte croissance offrant une plus grande mobilité pour les ordinateurs portables et les ordinateurs de poche. Du fait de sa disponibilité accrue et des économies qu'il engendre, l'Internet est de plus en plus employé pour les VPN d'accès à distance, utilisant à la fois l'accès commuté et l'accès direct. La Figure III.1 donne un exemple de sécurisation de l'accès à distance.

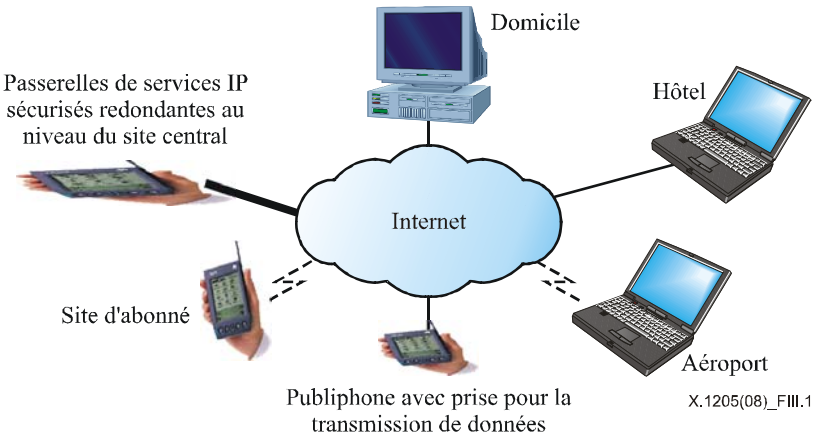

Figure III.1 – Sécurisation de l'accès à distance

Compte tenu des techniques exposées dans la présente Recommandation, on peut prendre les mesures suivantes pour sécuriser l'accès à distance:

1) *Accès commuté à un site d'entreprise centralisé*

Un utilisateur téléphonique distant établit un appel téléphonique depuis un modem connecté à son système informatique vers un groupe de modems (également appelé commutateur d'accès à distance) situé au niveau d'un site d'entreprise central ou régional. Les systèmes d'accès commuté devraient être configurés pour utiliser un système de gestion d'accès sécurisé assurant l'authentification et l'autorisation, comme décrit précédemment. L'accès commuté direct, largement utilisé dans les années 80 et au début des années 90, est maintenant rapidement remplacé par des VPN d'accès à distance fondés sur l'Internet.

2) *VPN d'accès à distance*

L'accès à distance fondé sur l'Internet offre une souplesse considérable et une grande largeur de bande. Il existe deux solutions: VPN fondés sur IPSec utilisant des clients VPN d'accès à distance ou VPN fondés sur SSL utilisant la capacité SSL du navigateur de l'utilisateur.

3) *VPN fondés sur IPSec*

Le protocole IPSec est une solution de couche réseau qui peut être utilisée pour diverses applications (par exemple si une connexion VPN fondée sur IPSec est établie, l'utilisateur peut accéder à la messagerie électronique et aux applications en libre-service, naviguer dans le réseau interne et accéder aux applications autorisées). Un client IPSec doit être chargé dans l'équipement d'utilisateur pour pouvoir être utilisé pour l'accès à distance. Des clients sont également disponibles pour les ordinateurs de poche. Un logiciel antivirus devrait aussi être chargé dans l'équipement d'utilisateur.

Qu'il soit fondé sur un accès commuté à un point de présence de fournisseur d'accès à l'Internet ou sur un accès direct filaire ou sans fil, le client VPN authentifie l'utilisateur, vérifie l'intégrité du système informatique de l'utilisateur et établit une liaison ou un tunnel sécurisé avec l'entreprise. Le client VPN offre des capacités (par exemple des pare-feu) permettant de garantir que le système distant proprement dit est sécurisé, en particulier pendant l'établissement de connexion avec l'entreprise. Pendant la phase d'établissement de session, le trafic avec l'entreprise fait l'objet d'un chiffrement et d'une authentification.

Les VPN d'accès à distance sont supposés pouvoir détecter et, si possible, contourner les obstacles courants de l'Internet comme les dispositifs NAT et les pare-feu en sortie (établissement d'une liaison vers le réseau de l'entreprise depuis l'intérieur d'un autre réseau protégé par un pare-feu) ou au moins fournir à l'utilisateur distant des informations sur la nature des obstacles rencontrés.

Côté entreprise, les connexions d'accès à distance depuis l'Internet sont gérées par un système de passerelles IPSec. L'entreprise devrait assurer une protection contre les défaillances ponctuelles en employant plusieurs passerelles avec plusieurs trajets vers l'Internet. Suivant l'étendue de l'entreprise, il est également recommandé de séparer géographiquement les passerelles. Celles-ci devraient prendre en charge un certain nombre de fonctionnalités pour assurer un accès à distance effectif dans toute l'entreprise. Les fonctionnalités recommandées sont les suivantes: configuration de client simple, capacité de faire passer des connexions par le réseau interne de l'entreprise par opposition à la terminaison de session et capacité d'assurer une fonctionnalité de pare-feu à états pour éviter la nécessité de disposer d'un pare-feu distinct. Par ailleurs, il est recommandé que la passerelle utilise divers mécanismes d'authentification (par exemple RADIUS, PKI et LDAP) afin de ménager une certaine souplesse dans le choix du niveau d'authentification de l'utilisateur. La passerelle devrait permettre à l'entreprise d'intégrer d'autres méthodes qui sont peut-être déjà utilisées, par exemple RADIUS, identité d'utilisateur fondée sur un annuaire/mot de passe, voire une authentification par carte à puce ou jeton sur les ordinateurs portables des utilisateurs. La prise en charge des protocoles L2TP et PPTP est utile.

III.2 Sécurisation de la téléphonie IP

Les organisations et les entreprises commencent à déployer des solutions de téléphonie IP, le but étant de tirer parti des avantages de la convergence dans les réseaux locaux et étendus ainsi que des applications intégrées. Chaque système de VoIP est une solution matérielle/logicielle qui comporte quatre fonctions logiques:

- Téléphones IP et clients logiciels sur PC.
- Serveurs de communication (également appelés portiers ou serveurs de gestion d'appel).

- Passerelles de média assurant un accès souple au réseau (par exemple par le biais des autocommutateurs privés classiques et du réseau téléphonique public commuté (RTPC) ainsi que du réseau public sans fil et au-delà).
- Serveurs d'application (par exemple messagerie unifiée, conférences et applications collaboratives fondées sur SIP).

Ces fonctions ainsi que les serveurs d'application de communication connexes tels que ceux qui prennent en charge les centres de contacts et la messagerie unifiée sont répartis dans un réseau IP de qualité téléphonique ou commerciale, qui offre les niveaux nécessaires de fiabilité, de qualité vocale et de gestion des encombrements. L'extension de la portée et de la mobilité est assurée sur les réseaux locaux sans fil et sur l'Internet via des VPN IP.

La Figure III.2 présente une solution type utilisée par une organisation pour sécuriser la téléphonie IP.

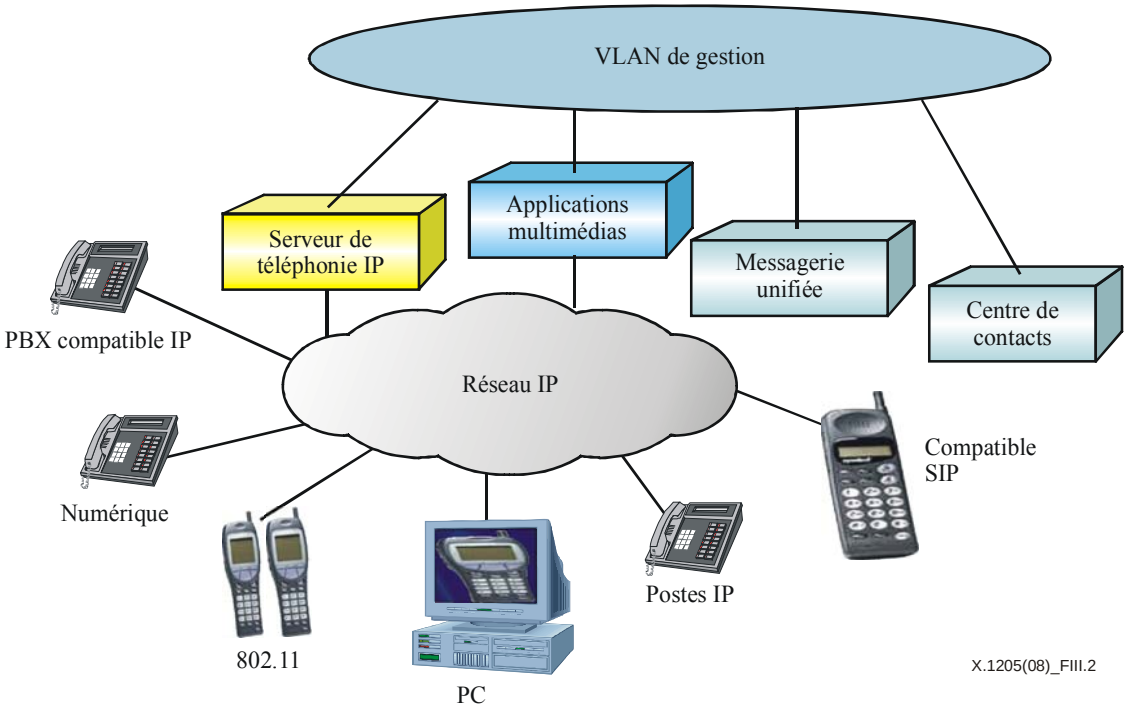

Figure III.2 – Sécurisation de la téléphonie IP

La téléphonie IP est une application qui fonctionne sur le réseau IP et tire parti de la fonctionnalité de sécurité assurée par un réseau. A la différence de la plupart des applications de données, la téléphonie IP est sensible au facteur temps et est essentielle pour la conduite des activités des entreprises. Tout comme les autres applications de données, les systèmes de téléphonie IP peuvent être confrontés à un certain nombre d'attaques. Par exemple:

- Les attaques visant un routeur peuvent mettre hors fonction à la fois les services vocaux et de données dans une organisation.
- Le déni de service peut entraîner la surcharge d'un client ou d'un serveur de communications téléphoniques IP.
- Le ping de la mort peut entraîner l'interruption des opérations de VoIP par l'envoi de plusieurs pings à des dispositifs de VoIP.
- L'analyse de ports peut entraîner la détection de vulnérabilités dans les clients et serveurs VoIP.

- Le reniflage de paquets peut entraîner l'enregistrement et/ou l'interception des conversations.
- L'usurpation d'adresse IP peut entraîner une mauvaise représentation de l'origine ou de la destination d'un flux de média ou de signalisation.
- Les virus, vers, chevaux de Troie et bombes à retardement peuvent attaquer serveurs et clients.

La téléphonie IP peut être compromise. Il existe des cas dans lesquels des pirates ont pris le rôle de clients IP, par exemple en raison d'un défaut d'administration des mots de passe ou de vulnérabilités associées au langage XML utilisé (cf. [b-W3C XML 1.0]). Ces attaques peuvent constituer une véritable menace lorsque la VoIP est utilisée de façon native sur l'Internet et une menace moindre lorsque la téléphonie IP est utilisée strictement à l'intérieur de l'entreprise et dans des connexions tunnellisées sur l'Internet.

Comme pour toute autre application, il faut, pour la téléphonie IP, procéder à une évaluation des risques pour estimer la valeur intrinsèque, comprendre les incidences des pertes à l'intérieur de l'organisation et formuler une politique de sécurité. La téléphonie est une fonction essentielle de l'entreprise et, tout comme le réseau, l'ensemble du système de téléphonie devra donc être protégé contre les menaces et les attaques visant la sécurité.

Généralement, les utilisateurs téléphoniques s'authentifient pour l'accès hors réseau au moyen d'un ensemble de fonctionnalités appelé accès direct au système (DISA). En revanche, il n'est pas rare que les utilisateurs de données soient tenus d'utiliser plusieurs identités d'utilisateur et mots de passe pour l'accès aux réseaux et aux applications. Cette complexité va à l'encontre de la sécurisation de l'environnement de l'entreprise. La simplicité sera encore plus importante avec la VoIP, étant donné que l'on souhaite une tonalité de numérotation instantanée. Il va sans dire que les différents mécanismes de sécurité de la VoIP ne doivent pas entraver la connectivité et la qualité vocale nécessaires.

Les principales lignes directrices concernant la sécurisation de la téléphonie IP sont les suivantes:

1) Les solutions de téléphonie IP d'entreprise sont utilisées dans les limites de l'entreprise, l'interfonctionnement avec le réseau public étant assuré sur des connexions à commutation de circuit.
2) Les systèmes de téléphonie IP d'entreprise nécessitent que l'infrastructure de réseau IP soit sécurisée du point de vue des données et qu'elle soit définie et conçue pour respecter les exigences de latence et de fiabilité de la téléphonie.
3) Les serveurs de communications téléphoniques IP d'entreprise sont essentiels pour les activités de l'entreprise et sont sécurisés sur le plan physique et protégés contre toute attaque interne ou externe.
4) Une authentification sécurisée des clients VoIP est assurée.
5) Le chiffrement de la voix n'est obligatoire que pour la traversée d'un réseau local à médias partagés ou sur l'Internet.
6) Une approche globale de la sécurité est adoptée dans l'ensemble de l'environnement téléphonique, qui englobe les clients et les serveurs VoIP, les serveurs d'application (par exemple pour la messagerie unifiée et les centres de contacts) et les autocommutateurs privés classiques.

Les solutions de sécurisation de la téléphonie IP nécessitent une approche coordonnée dans toutes les couches de réseau. La gestion de politique et la gestion d'accès sécurisée garantissent une authentification des utilisateurs et permettent de contrôler les fonctionnalités et les capacités d'appel de la téléphonie IP. Il convient d'utiliser des techniques de gestion sécurisée pour protéger les dispositifs de VoIP tels que les serveurs de communications et les passerelles de média. Les mécanismes de sécurité qui ont été mis en place pour les données peuvent être exploités pour la

VoIP: on peut par exemple utiliser IPsec pour l'accès à distance sécurisé, la connectivité des succursales et l'accès depuis des réseaux locaux sans fil. La gestion de politique peut permettre de renforcer la sécurité grâce à l'ajout d'une fonctionnalité d'inspection à états de la VoIP dans les pare-feu et d'une fonctionnalité de traduction d'adresse réseau. La sécurité des applications peut être assurée de diverses façons, notamment par le renforcement des systèmes d'exploitation et par une protection antivirus installé dans l'équipement d'utilisateur.

III.2.1 Sécurisation des serveurs d'application et des serveurs de communications téléphoniques IP

Le cœur du système de téléphonie IP est le serveur de communications, qui peut être autonome ou intégré avec un gestionnaire de communications d'entreprise PBX compatible IP. Sont également importants les serveurs d'application prenant en charge des centres de contacts, des applications multimédias, la messagerie unifiée et les systèmes à réponse vocale interactive en autoservice. Pour sécuriser ces serveurs, il faut commencer par renforcer les systèmes d'exploitation comme décrit.

III.2.2 Sécurisation des clients VoIP

Les solutions de VoIP prennent en charge une grande diversité de clients et de configurations d'accès, notamment des téléphones filaires ou sans fil IP et des clients logiciels sur PC. Lorsque ces clients sont connectés à un réseau IP, ils sont vulnérables aux attaques.

Pour la téléphonie, il existe différents protocoles de signalisation (par exemple SIP). Le trafic de signalisation utilise généralement le protocole TCP au niveau du transport. A l'avenir, il sera largement possible de sécuriser le trafic de signalisation au niveau du client VoIP. Dans les systèmes de téléphonie IP, le signal vocal est mis en paquets selon une norme telle que le document [b-UIT-T G.729] (à 8 kbit/s) et un algorithme de détection de l'activité vocale et on utilise le protocole de transport en temps réel (RTP) avec le protocole UDP au niveau du transport.

Il existe de grandes différences dans les modalités de réduction des risques pour les téléphones IP et pour les clients de téléphonie logicielle sur PC. Les téléphones IP sont des appareils destinés exclusivement à la téléphonie. Ils n'ont pas de mémoire ou d'actif à protéger (seule doit être protégée la présence de ces téléphones dans le réseau en tant que dispositifs sécurisés). L'identification de l'appelant et l'appel proprement dit sont les seuls actifs à protéger. Ces appareils téléphoniques utilisent le plus souvent un protocole client léger propriétaire qui s'appuie sur le serveur de communications pour ce qui est des fonctionnalités et de la sécurité. Cette approche est différente des mises en œuvre qui s'appuient sur le langage XML dans le téléphone VoIP pour l'exploitation des fonctionnalités, ce qui peut être à l'origine de vulnérabilités.

Les clients logiciels VoIP résident dans les équipements d'utilisateur avec d'autres applications et d'autres actifs, et sont fondés sur des systèmes d'exploitation couramment utilisés. Une attaque qui aboutit peut coûter cher, étant donné que les équipements d'utilisateur comportent de nombreux actifs précieux (applications, données commerciales, financières et personnelles). La pratique courante consiste à utiliser une ou plusieurs applications de sécurité conçues pour les plates-formes d'équipement d'utilisateur, prenant en charge des pare-feu personnels, des systèmes antivirus et des clients VPN IP. Pour les clients logiciels VoIP, on peut utiliser les mêmes mécanismes que ceux qui s'appliquent dans le cas des données.

III.2.3 Sécurisation de la VoIP dans l'armoire de répartition et à travers le campus

Il existe deux façons de câbler les dispositifs IP dans un réseau de campus: Ethernet à médias partagés et Ethernet commuté spécialisé. L'industrie s'oriente généralement vers l'Ethernet commuté spécialisé, compte tenu de la croissance du trafic et des exigences en matière de gérabilité. Par ailleurs, la sécurité et la gérabilité sont également à l'origine du déploiement de VLAN (cf. [b-ISO/CEI 18028-5]) dans les réseaux d'entreprise. Les réseaux locaux sans fil constituent une troisième solution, qui est de plus en plus souvent mise en œuvre dans des environnements comme l'enseignement et les soins de santé.

Avec l'introduction de la téléphonie IP, il est fortement recommandé que les clients logiciels VoIP et les appareils de VoIP soient raccordés à des environnements Ethernet commutés tout près du bureau, ce qui permet de respecter les exigences suivantes:

– La variation de latence de la VoIP est réduite au minimum grâce à la suppression de l'exploitation CDMA dans le cadre de l'Ethernet à médias partagés.
– On améliore la sécurité de la VoIP en empêchant aux autres bureaux de pouvoir écouter de façon clandestine les appels de VoIP.

En outre, les entreprises peuvent choisir de regrouper logiquement les téléphones VoIP dans leurs propres VLAN afin de faciliter la gérabilité.

La téléphonie IP peut améliorer considérablement la productivité des utilisateurs raccordés à des réseaux locaux sans fil (WLAN) dans l'entreprise, en étendant les fonctionnalités de téléphonie du bureau vers, par exemple, une salle de conférence ou une salle informatique. En raison de la nature hostile de ces WLAN, il est recommandé, sur le plan de l'architecture, de sécuriser à la fois le plan de signalisation et le plan vocal sur le segment sans fil. Pour cela, on peut configurer les clients logiciels de manière à ce qu'ils résident au même endroit qu'un client VPN IP sur un ordinateur portable. Une autre solution consiste à intégrer un chiffrement et une authentification dans les téléphones IP de WLAN. Les deux solutions offrent une authentification d'utilisateur et un chiffrement robustes pour les environnements WLAN.

III.2.4 Sécurisation des succursales pour la téléphonie IP

Il existe différentes méthodes pour prendre en charge des solutions de VoIP dans les bureaux distants et dans les succursales. Des téléphones et des clients logiciels VoIP peuvent par exemple être pris en charge dans le cadre de solutions globales ("*office-in-a-box*"). D'autres méthodes exploitent complètement la nature répartie de la VoIP en déployant des clients en dehors d'un serveur centralisé. Dans tous les cas, il est recommandé que le trafic de VoIP dans la succursale soit acheminé de façon sécurisée sur un VPN IP établi pour les données.

III.2.5 Sécurisation de l'accès à distance pour la téléphonie IP

La téléphonie IP peut améliorer considérablement la productivité des utilisateurs distants, qu'ils travaillent à leur domicile, depuis un hôtel ou sur la route, dans tous les cas en étendant les fonctionnalités de téléphonie du bureau vers l'emplacement distant. Des clients logiciels VoIP résideraient au même endroit qu'un client VPN IP sur un ordinateur portable pour les employés qui sont très mobiles. C'est cette même configuration qui serait utilisée pour tirer parti des points d'accès WLAN dans les hôtels, les aéroports et les centres de congrès. Des téléphones VoIP offriraient de nombreuses fonctionnalités de communications aux télétravailleurs et aux agents de centres de contacts, la sécurité étant assurée par un VPN IP.

III.2.6 Sécurité de la gestion de réseau pour la téléphonie IP

Du point de vue de la gestion, il convient de configurer un port Ethernet dédié physiquement. Ce port devrait faire partie d'un VLAN de gestion, l'ensemble du trafic autre que de gestion étant bloqué au niveau du routage au moyen de listes d'accès et d'une protection périmétrique. L'accès externe des fournisseurs, des intégrateurs de système et/ou des revendeurs à valeur ajoutée peut être fourni par le biais de VPN IP. Les ports inutilisés (par exemple pour les consoles ou l'accès à distance par un modem) devraient être désactivés. Seuls les logiciels d'application autorisés devraient fonctionner sur ces serveurs. Il convient d'utiliser une sécurité multiniveaux, avec divers niveaux de privilèges (surveillance, configuration, commande) pour le personnel d'exploitation authentifié. Les mots de passe des utilisateurs sont stockés en toute sécurité et la gestion du formatage et de la modification des mots de passe sont contrôlées de façon stricte. Le trafic de gestion (par exemple les informations de facturation) peut facultativement être chiffré, y compris pour la transmission interne, par le biais de la technologie VPN IP.

III.3 Sécurisation des bureaux distants

Un bureau distant peut être de n'importe quelle taille, allant du bureau d'un télétravailleur à un grand campus d'entreprise. Un "bureau distant" et un "accès à distance" ont de nombreux éléments en commun, mais ils se distinguent par la persistance des capacités de communication bidirectionnelles entre l'emplacement distant et le reste de l'entreprise. Autrement dit, un bureau distant est un lieu de travail, qui est raccordé en permanence au reste de l'entreprise et est capable d'échanger des messages avec le reste de l'entreprise pendant les heures de travail. Quant à l'accès à distance, il s'agit d'une connexion temporaire à l'entreprise établie sur demande par le ou les utilisateurs qui accèdent à distance.

La mise en réseau des succursales, qui est onéreuse, est l'élément fondamental pour la fourniture de services dans bon nombre de secteurs (par exemple services bancaires au public, soins de santé et services publics). Les environnements classiques de mise en réseau des succursales sont fondés sur diverses technologies de réseau local et sur des routeurs multiprotocoles, fonctionnant dans des réseaux en relais de trame avec secours à commutation de circuit RNIS. Quatre évolutions importantes offrent des possibilités importantes de transformation de la mise en réseau des succursales: 1) la convergence sur Ethernet en tant que norme pour les réseaux locaux; 2) l'acceptation universelle du protocole IP en tant que protocole préféré; 3) l'Internet; et 4) une liste croissante de services VPN de couches 2 et 3. Toutefois, ces évolutions posent aussi divers problèmes de sécurité, notamment pour les grandes entreprises. On trouvera une illustration sur la Figure III.3.

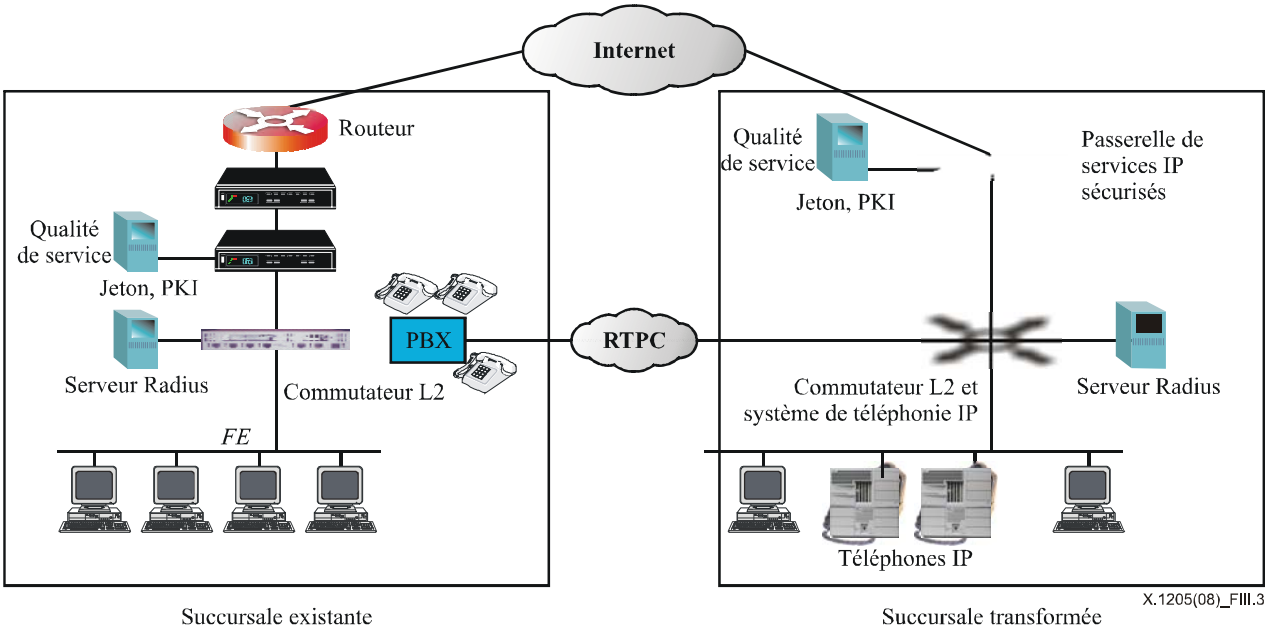

Figure III.3 – Sécurisation des bureaux distants

Les exigences en périphérie de WAN au niveau d'une succursale incluent le routage entre VLAN localement et dans le réseau, la gestion de la qualité de service et de la largeur de bande et un interfaçage évolutif dans le réseau WAN. Pour cela, il faut notamment prendre en charge un mécanisme d'encapsulation sur le WAN et le niveau de fiabilité approprié. Il est essentiel d'assurer une sécurité rentable sur l'Internet (et même sur relais de trame). Gérer la transition entre les technologies WAN existantes relativement sécurisées et les VPN IP est également une tâche ardue. Certaines entreprises souhaitent offrir un accès à l'Internet direct depuis chaque bureau distant, d'où la nécessité d'installer des pare-feu distants. D'autres souhaitent une connectivité à routage dynamique très fiable entre les succursales et le réseau dorsal de l'entreprise, avec des pare-feu

centralisés dans l'Internet, utilisant dans certains cas le relais de trame pour le trajet principal et l'Internet pour le secours, ou passant à des VPN IP comme configuration principale. Le routage dynamique sert à améliorer l'évolutivité et la fiabilité grâce à:

- un apprentissage automatique de la topologie du réseau;
- un apprentissage automatique des adresses des utilisateurs finals dans l'entreprise;
- une adaptation automatique aux changements de topologie du réseau.

Toutefois, dans les réseaux à routage dynamique, on ne s'est intéressé à la sécurité qu'après coup et non dès le départ. Par exemple, il n'existe pas de moyen efficace de procéder à un routage dynamique sur des tunnels chiffrés dans le cadre de VPN, et la gestion de ces tunnels s'avère difficile.

D'une manière générale, les considérations ci-dessus ont conduit les entreprises à procéder à l'achat, à l'installation, à la maintenance et à la gestion de plusieurs dispositifs de sécurité et de mise en réseau pour les bureaux distants et les succursales, ce qui a conduit à une certaine complexité et à des coûts de gestion élevés.

Avec le passage aux VPN IP sur l'Internet, un ensemble complet d'exigences de sécurité doit être respecté et ce, le plus rentablement possible. Il s'agit d'assurer des fonctions de sécurité de réseau comme le routage IP sur des tunnels sécurisés, l'établissement de réseaux privés virtuels (VPN), le chiffrement, l'inspection à états dans les pare-feu au niveau de la couche de réseau, l'authentification des bureaux distants et des services d'annuaire au niveau de la couche de gestion d'accès sécurisée, toutes ces fonctions devant être fortement intégrées. La gestion de la politique de sécurité doit être intégrée à cette solution, permettant à chaque utilisateur d'être configuré avec un profil de sécurité unique, qui reste avec l'individu, que celui-ci se connecte depuis un équipement d'utilisateur à son domicile par le biais de l'Internet public ou qu'il se connecte localement à l'intérieur de la succursale. La sécurité de gestion du réseau doit aussi être étendue aux bureaux distants, sans portes dérobées qui pourraient porter atteinte à la sécurité du réseau. Enfin, il faut assurer la sécurité des applications si des serveurs de données et/ou la téléphonie IP sont déployés dans des bureaux distants.

III.4 Sécurisation des WLAN

Les possibilités de communication entre le siège d'une entreprise, ses succursales, les employés distants, les consultants et les partenaires commerciaux évoluent. Les entreprises peuvent maintenant exploiter les nouvelles technologies sans fil IEEE 802.11 (cf. [b-IEEE 802.11]) pour conduire leurs activités à tout moment et en tout lieu. Toutefois, ces solutions débouchent sur la double nécessité d'une gestion centrale et efficace de l'accès des utilisateurs et de la sécurisation des ressources d'une organisation.

Les WLAN sont particulièrement vulnérables aux atteintes à la sécurité. L'interception de communications sur un réseau local standard nécessite un accès physique à l'infrastructure de câblage. En revanche, les transmissions sans fil peuvent faire l'objet d'une interception hertzienne et exposent le réseau à des intrusions de la part de n'importe quelle personne ayant une carte de réseau local sans fil standard.

Les WLAN élargissent le réseau de l'entreprise en utilisant des dispositifs sans fil et le protocole IEEE 802.11. Les équipements des WLAN comportent des cartes d'interface de réseau (NIC) sans fil pour les équipements mobiles comme les ordinateurs portables et les ordinateurs de bureau, appelés unités mobiles (MU) ou stations (STA). Les cartes NIC permettent aux signaux d'être acheminés dans le réseau depuis le dispositif de connexion en passant par un dispositif intermédiaire, la passerelle de réseau local sans fil, ou un pivot appelé point d'accès sans fil, qui convertit les signaux hertziens en signaux à acheminer sur le réseau filaire.

Grâce à un pivot ou à un commutateur Ethernet, les entreprises peuvent raccorder les points d'accès de réseau local sans fil au réseau local filaire aussi facilement que l'ajout d'un utilisateur filaire. Le raccordement des points d'accès à un commutateur permet de garantir à chaque point d'accès une liaison dédiée à 10/100 Mbit/s, ce qui permet à tous les points d'accès disponibles de se comporter comme un commutateur et de ne pas avoir à faire face au problème de l'obtention d'une partie de la largeur de bande du pivot filaire.

La norme [b-IEEE 802.11] initiale est une famille de spécifications, dont les spécifications IEEE 802.11a, IEEE 802.11b, IEEE 802.11g et IEEE 802.11i sont actuellement disponibles. Elle est utilisée sur la base de l'environnement des signaux dans le réseau, avec des compromis entre la distance et la largeur de bande.

III.4.1 Problèmes de sécurité dans les WLAN

Dans les WLAN, quels que soient les mécanismes de sécurité utilisés, les signaux sont radiodiffusés et reçus via des ondes radioélectriques et il n'y a donc pas de barrière physique aux utilisateurs non autorisés. Ces signaux peuvent malheureusement faire l'objet d'interceptions et conduire à des intrusions dans le réseau de l'entreprise. Par conséquent, si on veut ajouter un nœud sans fil dans le réseau d'une entreprise, il faut respecter certaines précautions et bonnes pratiques de sécurité afin de protéger l'ensemble des actifs du WLAN.

La couche infrastructure d'un WLAN comporte tous les éléments du réseau, câbles, supports d'interconnexion et de transmission (couverture), par exemple points d'accès, stations mobile, passerelles et serveurs hébergeant des services associés tels que RADIUS, DNS, etc.

La couche services est composée des services d'accès au WLAN et d'autres services associés, par exemple le service d'authentification, autorisation et comptabilité (AAA), le service de gestion de clés, etc.

Les menaces de sécurité posées par les WLAN sont notamment les suivantes:

- Atteintes à la confidentialité et à l'intégrité du trafic sans fil. Un attaquant peut intercepter des communications entre un ordinateur mobile et un point d'accès sans fil, et ainsi obtenir des informations sensibles ou classées qui ne sont pas destinées à un tiers. Il peut aussi insérer des informations dans une transaction authentique, sans que les utilisateurs légitimes en aient connaissance.
- Exposition des réseaux locaux d'entreprise. Si les plates-formes mobiles ne sont pas authentifiées de façon sécurisée, un attaquant peut simplement se raccorder au WLAN en utilisant un dispositif conforme à la norme IEEE 802.11 et devenir une station "autorisée" sur le WLAN, ce qui lui permet d'accéder au réseau local d'entreprise.

Sur la base du modèle de menaces X.800, les attaques peuvent être récapitulées comme suit:

Modèle de menaces X.800	Méthodes d'attaque
Destruction d'informations et/ou d'autres ressources	Intrusion à un point d'accès
Corruption ou modification d'informations	Craquage de clés WEP, attaque par intercepteur
Vol, suppression ou perte d'informations et/ou d'autres ressources	Intrusion à un point d'accès, craquage de clés WEP, attaque par intercepteur, usurpation d'adresse MAC, dispositifs indésirables, War driving, détournement de couche 3, réseaux ad hoc

Modèle de menaces X.800	Méthodes d'attaque
Divulgation d'informations	Intrusion à un point d'accès, craquage de clés WEP, attaque par intercepteur, usurpation d'adresse MAC, dispositifs indésirables, War driving, détournement de couche 3, réseaux ad hoc
Interruption de services	Brouillage radioélectrique, inondation de données, détournement de couche 2, faux point d'accès, usurpation de trame de désauthentification, attaque DoS FATA-Jack

Tout comme les réseaux filaires, les WLAN doivent prendre en charge la confidentialité, l'intégrité et des contrôles d'accès. Le principal problème de sécurité avec le sans fil est que les personnes externes peuvent facilement recevoir ou transmettre en provenance et à destination du WLAN, qu'elles soient considérées ou non comme étant hors de portée.

Ainsi les attaquants peuvent procéder à des écoutes clandestines et insérer des points d'accès non autorisés (appelés points d'accès indésirables) pour lancer des attaques (par exemple des attaques par intercepteur ou un détournement de session) et attaquer facilement les utilisateurs WLAN depuis l'intérieur du WLAN. Un attaquant peut alors tromper un utilisateur en le faisant se connecter au point d'accès de l'attaquant, qui se comporte comme un nœud légitime sur le réseau, et peut alors partager librement et à l'insu de l'utilisateur des identités d'utilisateur, des mots de passe et d'autres informations privées.

On peut utiliser les techniques suivantes pour sécuriser l'environnement sans fil:

- Noms de réseau: identificateurs d'ensemble de services (SSID).
- Enregistrement de carte: listes de contrôle d'accès (ACL) MAC.
- Chiffrement à clé partagée: utilisation de protocoles de sécurité (par exemple WPA/WPA2).

En outre, les types d'authentification suivants peuvent être utilisés:

- Authentification en système ouvert: permet à quiconque possédant l'identificateur SSID du point d'accès d'obtenir un accès.
- Authentification à clé partagée: l'authentification de l'utilisateur est fondée sur le secret partagé qu'il possède.

Dans la spécification [b-IEEE 802.11] initiale, la sécurisation de l'itinérance est assurée par la préauthentification de l'unité mobile auprès des points d'accès environnants. Il n'y a pas de message de transfert entre points d'accès, étant donné que l'ensemble des points d'accès et des unités mobiles utilisent la même clé partagée, permettant au nouveau point d'accès de supposer que l'authentification de l'unité mobile est valable. Ainsi le transfert est rapide mais l'authentification est moins sûre car les trames de gestion ne sont pas authentifiées.

III.4.2 Exigences et mécanismes de sécurité à l'entrée et à l'intérieur du point d'accès sans fil

La seule façon de protéger réellement l'environnement sans fil, qui par nature est ouvert, consiste à adopter des solutions cryptographiques et des mesures d'authentification appropriées qui valident l'utilisateur final. Le trafic est chiffré au niveau d'une passerelle dont l'identificateur peut être validé sur le plan cryptographique.

Pour qu'un WLAN soit sécurisé, les deux principales exigences concernent la sécurisation du trafic et la sécurisation de l'itinérance. Concernant la sécurisation des communications, il faut avant tout chiffrer le trafic allant du dispositif mobile au point d'accès, à une passerelle située derrière le point d'accès (par exemple utilisant une passerelle IPSec) ou au serveur d'application (site web sécurisé). Concernant la sécurisation de l'itinérance, les utilisateurs mobiles doivent pouvoir passer d'un point d'accès à un autre sans perdre leurs sessions actives et sans avoir à s'authentifier une nouvelle fois auprès du nouveau point d'accès. Le passage d'un point d'accès à un autre est assujetti à des

contraintes temporelles strictes pour que l'incidence sur l'application de l'utilisateur soit minimale. Les utilisateurs comptent sur une protection correcte de leurs justificatifs d'identité lorsque ceux-ci sont transférés d'un domaine à un autre.

III.4.3 Améliorations de la spécification IEEE 802.11 en matière de sécurité

Les risques de sécurité susmentionnés conduisent à des améliorations de la norme [b-IEEE 802.11] initiale afin de sécuriser plus efficacement les réseaux locaux sans fil. La norme IEEE 802.11i présente le contrôle d'accès IEEE 802.1X (cf. [b-IEEE 802.1X]), le recalcul dynamique de clé, des mécanismes de distribution de clé par session et des algorithmes cryptographiques forts. Le document [b-IEEE 802.1X] définit une authentification et un contrôle d'accès poussés pour les points d'accès grâce à l'utilisation du protocole d'authentification extensible (EAP), qui est un ensemble de messages de négociation et de transport de l'authentification entre client et serveur (cf. [b-IETF RFC 2716], [b-IETF RFC 3748] et [b-IETF RFC 4017]). Le protocole EAP prend en charge plusieurs méthodes d'authentification, dont l'algorithme MD5 et le protocole de sécurité de la couche transport (TLS), l'algorithme MD5 étant la méthode la plus largement disponible et prise en charge. Indépendamment du choix du protocole EAP, les trois composants IEEE 802.1X (cf. [b-IEEE 802.1X]) doivent prendre en charge la même méthode (cf. Figure III.4.3).

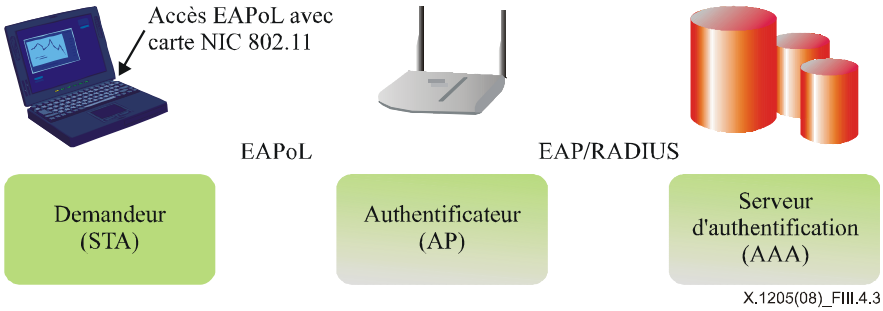

Figure III.4.3 – Composants IEEE 802.1X

Pour sécuriser l'itinérance IEEE 802.1X, l'utilisateur doit toujours s'authentifier à nouveau auprès du nouveau point d'accès. Les clés par session et la lenteur des opérations liées à l'infrastructure de clé publique (PKI) font qu'il est difficile de procéder à une nouvelle authentification rapide. Ces options d'authentification poseront donc quelques difficultés pour les transferts entre points d'accès en cas d'itinérance.

Dans le cadre du document [b-IEEE 802.1X], les protocoles EAP-TTLS et PEAP permettent de procéder à une nouvelle authentification rapide en cas d'itinérance et ce, en tirant parti du mécanisme de réétablissement de connexion pris en charge dans le protocole de prise de contact TLS. L'authentification complète n'est pas requise si on suppose que la connaissance du secret maître prouvée par la possibilité de reprendre la session TLS suffit pour l'authentification.

III.4.4 Approche par couches pour sécuriser les réseaux locaux sans fil

Pour que les architectures de WLAN soient correctement sécurisées, il faut adopter une approche par couches et appliquer plusieurs technologies, comme dans les environnements habituels de réseau local. La solution finale devrait être une architecture de sécurité WLAN/LAN intégrée. Chaque fois que c'est possible, les mécanismes de sécurité existants dans les réseaux locaux devraient être étendus pour s'appliquer aux WLAN.

III.4.4.1 Point d'accès

On peut utiliser des identificateurs ESSID et une liste ACL MAC, même s'ils offrent une sécurité très faible. L'ensemble des unités mobiles et des points d'accès configurés avec le même identificateur ESSID peuvent s'associer librement. Le document [b-IEEE 802.11] prend en charge

un "identificateur ESSID de diffusion", qui permet à une unité mobile de s'associer à un point d'accès sans connaître l'identificateur ESSID. La désactivation de cette fonctionnalité permet d'améliorer la sécurité. La liste ACL MAC contient la liste des adresses MAC autorisées et peut contenir la liste des adresses interdites, sachant que celle-ci devient difficile à gérer lorsque les ordinateurs en jeu sont nombreux.

Actuellement, on peut facilement mettre en œuvre des points d'accès prenant en charge les mécanismes de sécurité propriétaires ou prénormalisés suivants: WPA, WPA2, WEP dynamique, norme de chiffrement perfectionné (AES), protocole d'intégrité de clé temporelle (TKIP) et chiffrement par clé de 128 bits. Le protocole WEP dynamique permet de changer la clé WEP plus souvent, à des intervalles prédéterminés. La norme AES est la nouvelle norme approuvée par le FIPS (*federal information processing standard*) destinée à remplacer l'algorithme de chiffrement DES. Le protocole TKIP renforce l'algorithme de programmation des clés pour assurer la protection contre les attaques par récupération de clé en ce qui concerne le WEP classique. En raison de sa faiblesse, il est recommandé, dans le document [b-IEEE 802.11], de ne pas utiliser le protocole TKIP sauf en tant que correctif pour les anciens équipements.

NOTE – L'accès protégé Wi-Fi (WPA), qui était au départ une initiative de l'industrie, vise à améliorer la sécurité des réseaux locaux sans fil. WPA-PSK est un mode particulier d'accès WPA pour les utilisateurs résidentiels sans serveur d'authentification d'entreprise et assure une protection forte par chiffrement. Dans le mode WPA-PSK, les clés de chiffrement sont modifiées automatiquement (recalcul de clé) et authentifiées entre dispositifs après un délai spécifié ou après qu'un nombre de paquets spécifié a été transmis. Le mécanisme WPA-PSK utilise un secret partagé qui est introduit à la fois dans l'enveloppe extérieure du point d'accès sans fil et dans les clients WPA. La longueur du secret partagé peut être comprise entre 8 et 63 caractères. Le protocole d'intégrité de clé temporelle (TKIP) est utilisé après l'introduction du secret partagé initial dans les dispositifs sans fil et gère le chiffrement et le recalcul automatique de clé. Le mécanisme WPA est conçu comme une mise à niveau logicielle. D'après les fournisseurs de produits sans fil et les professionnels de la sécurité, les mécanismes WPA et WPA-PSK actuels devraient être utiles très longtemps. Dans le cadre de l'accès WPA, l'utilisation de la norme de chiffrement perfectionné (AES) est définie comme une alternative facultative au chiffrement WEP.

III.4.4.2 Espace aérien

Avec une antenne directive de gain élevé, une personne externe qui est située à plusieurs kilomètres d'un WLAN et qui souhaite accéder de façon non autorisée à ce réseau peut parvenir à ses fins. Il serait préférable de l'en empêcher. Pour empêcher les personnes externes non autorisées de tirer parti de la disponibilité du signal dans l'atmosphère en utilisant une antenne directive de gain élevé, une méthode consiste à entourer le périmètre de l'enceinte de l'entreprise ou le réseau WLAN, de points d'accès qui ne sont pas connectés au réseau interne (cf. Figure III.4.4.2). Une personne externe ne peut pas voir le WLAN interne car les points d'accès externes fonctionnent à la même fréquence porteuse que les points d'accès internes et offrent une intensité de signal plus élevée à la personne externe, "brouillant" le signal interne pour la personne externe. On peut améliorer cette configuration en raccordant les points d'accès externes à un réseau isolé et en ajoutant un système de détection des intrusions (IDS) et un pot de miel pour la détection des intrusions et la collecte de preuves.

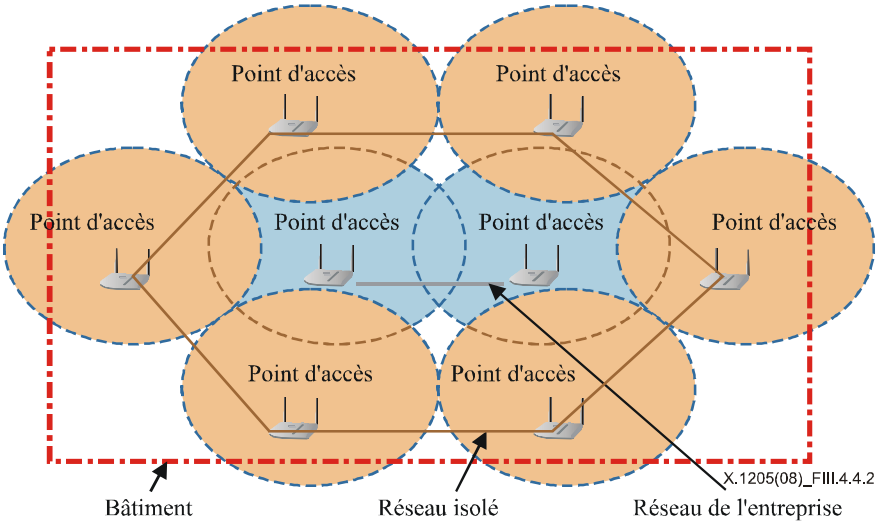

Figure III.4.4.2 – Points d'accès sentinelles pour la sécurité périmétrique

III.4.4.3 Segmentation

Chaque fois que c'est possible, les mécanismes de sécurité existants dans les réseaux locaux devraient être étendus afin de s'appliquer aux WLAN. Des mécanismes supplémentaires comme le chiffrement basé sur des VPN et le protocole TLS, la segmentation des segments sans fil par le biais de réseaux locaux virtuels (VLAN) et la défense périmétrique au moyen d'un pare-feu sont efficaces, indépendamment des améliorations supplémentaires apportées au document [b-IEEE 802.1X]. La Figure III.4.4.3 présente des points d'accès IEEE 802.11 génériques de WLAN avec un identificateur SSID commun, constituant un sous-réseau raccordé à un commutateur de couche 2. Le commutateur de couche 2 peut limiter de façon intelligente le trafic allant vers d'autres points d'accès, certains pouvant être raccordés à des VLAN. Concernant les points d'accès se trouvant dans un autre sous-réseau (autre identificateur SSID), une connexion peut être établie par le biais d'un commutateur de routage de couche 2/3. Dans cette architecture, la sécurité des communications, la sécurité de l'itinérance et des transferts et la défense périmétrique sont considérées comme faisant partie de l'environnement de réseau WLAN/LAN sécurisé et intégré.

Le protocole IPSec est un protocole éprouvé et fiable pour la sécurisation des communications. Pour les environnements qui peuvent exploiter des clients IPSec sur des dispositifs mobiles ou qui peuvent avoir des applications avec plusieurs ordinateurs frontaux fondés sur le web, le protocole IPSec est la méthode la mieux adaptée pour sécuriser les communications. Le principal avantage d'un VPN IPSec est que l'entreprise a l'entière maîtrise de la politique de sécurité robuste de sorte que quelqu'un qui se raccorde à un réseau local dispose de tous les privilèges d'un utilisateur local du réseau local.

Les mêmes techniques s'appliquent à un WLAN utilisé pour un "point d'accès public". Par exemple, un employé à distance peut, depuis un hôtel, accéder à un fournisseur d'accès à l'Internet au moyen d'une ligne DSL en utilisant un client PPPoE et une identité d'utilisateur/un mot de passe fournis par l'hôtel. Il peut ensuite se raccorder au réseau de son entreprise en utilisant un client IPSec.

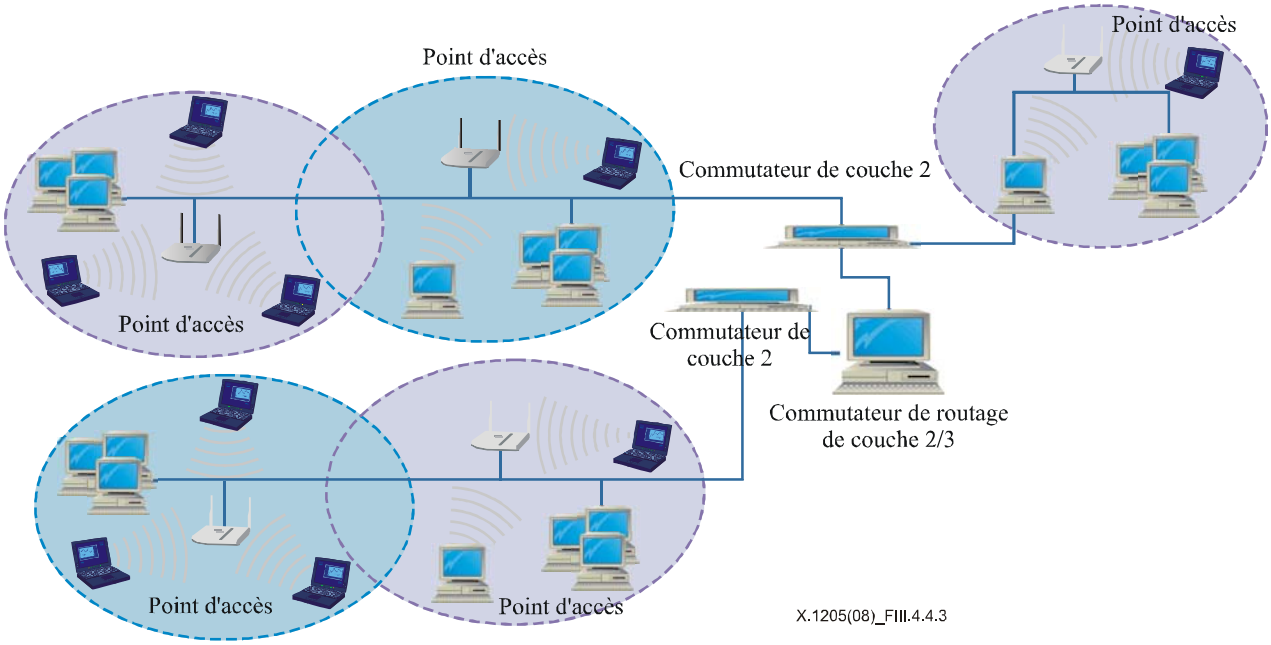

Figure III.4.4.3 – Points d'accès IEEE 802.11 génériques de WLAN avec un identificateur SSID commun

III.4.4.4 Couche de gestion

Il convient d'utiliser aussi des contre-mesures de gestion et d'exploitation pour sécuriser les WLAN, par exemple en étendant la politique de sécurité d'une organisation pour englober les WLAN. Chaque fois que c'est possible, les mécanismes de sécurité existants dans les réseaux locaux devraient être étendus pour s'appliquer aux WLAN; sinon, il faut intégrer de nouveaux mécanismes avec les mécanismes existants. Par exemple, la mise en œuvre de solutions IPSec permet à l'entreprise de procéder à une gestion centralisée des utilisateurs WLAN, des utilisateurs distants et des règles applicables aux pare-feu et ne nécessite pas d'application de gestion supplémentaire si cette gestion est déjà appliquée pour l'accès extranet. Les fournisseurs englobent désormais les WLAN dans le cadre des mécanismes tels que la découverte de réseau, les analyseurs de vulnérabilité et les systèmes IDS.

III.4.4.5 Analyse des protocoles d'accès aux WLAN

Les points forts et les points faibles relatifs des divers protocoles Wi-Fi examinés dans les paragraphes ci-dessus, à savoir IEEE 802.11i, WPA2[2], WPA et WEP, peuvent être analysés suivant les dimensions UIT-T X.805. L'analyse est présentée pour certaines des dimensions, mais elle peut être étendue à l'ensemble des huit dimensions.

Pour chaque dimension, les résultats qualitatifs sont présentés dans un tableau dont la légende est la suivante:

√	satisfaisant
P	partiel
X	non pris en charge dans la norme

[2] Les protocoles WPA2 et IEEE 802.11i présentent des caractéristiques de sécurité analogues, mais étant donné que le protocole WPA2 peut être exploité avec le protocole WPA qui est moins fiable, les points faibles du protocole WPA ont une incidence sur la sécurité du protocole WPA2.

Contrôle d'accès

Les spécifications [b-IEEE 802.11] initiales, incluant le protocole WEP, ne prévoyaient pas de mécanisme de contrôle d'accès intégré, de sorte que les vastes WLAN utilisaient une passerelle WLAN pour le contrôle d'accès au niveau des services. C'est pourquoi le contrôle d'accès a été noté comme étant partiellement adéquat dans le cas des services WLAN pour les utilisateurs finals.

Le document [b-IEEE 802.1X] définit le mécanisme de contrôle d'accès des utilisateurs finals pour les services Wi-Fi fondés sur les protocoles IEEE 802.11i, WPA et WPA2.

Tableau III.2 – Couverture pour la dimension contrôle d'accès

Dimension de sécurité: contrôle d'accès								
Plans de sécurité	**Couches de sécurité**							
	Infrastructure				**Services**			
	IEEE 802.11i	**WPA2**	**WPA**	**WEP**	**IEEE 802.11i**	**WPA2**	**WPA**	**WEP**
Utilisateur final	√	√	√	X	√	√	√	P
Commande	√	X	X	X	√	√	√	X
Gestion	X	X	X	X	X	X	X	X

Authentification

Les protocoles IEEE 802.11i, WPA2 et WPA utilisent l'authentification IEEE 802.1X/EAP. En revanche, le protocole WEP emploie une authentification "ouverte" ou "à secret partagé", qui utilise la même clé statique que celle qui est utilisée pour le chiffrement. L'authentification est donc notée comme étant "partielle" dans le cas du protocole WEP. Pour les autres protocoles, l'authentification pourrait aussi être notée de la même manière si un protocole EAP faible de type MD5 était choisi pour l'authentification [b-IEEE 802.1X].

L'authentification des informations de commande aux points d'accès et dans les autres éléments de réseau (pour assurer l'itinérance) n'est prise en charge que dans la norme IEEE 802.11i. Les points d'accès fondés sur les autres normes utilisent généralement des mécanismes propriétaires pour échanger ces informations en cours d'itinérance et la validation de la sécurité de ces mises en œuvre n'entre pas dans le cadre de la présente analyse.

Tableau III.3 – Couverture pour la dimension authentification

Dimension de sécurité: authentification								
Plans de sécurité	**Couches de sécurité**							
	Infrastructure				**Services**			
	IEEE 802.11i	**WPA2**	**WPA**	**WEP**	**IEEE 802.11i**	**WPA2**	**WPA**	**WEP**
Utilisateur final	√	√	√	P	√	√	√	P
Commande	√	X	X	X	√	√	√	X
Gestion	X	X	X	X	X	X	X	X

Disponibilité

Les attaques DoS de type brouillage radioélectrique, inondation de données et détournement de session de couche 2, sont toutes des attaques contre la disponibilité. Les normes de sécurité des WLAN ne peuvent pas empêcher les attaques contre la couche physique, tout simplement parce qu'elles s'appliquent au niveau de la couche 2 et au-dessus. De même, elles sont inutiles en cas de défaillance d'un point d'accès.

Tableau III.4 – Couverture pour la dimension disponibilité

Dimension de sécurité: disponibilité								
Plans de sécurité	**Couches de sécurité**							
	Infrastructure				**Services**			
	IEEE 802.11i	**WPA2**	**WPA**	**WEP**	**IEEE 802.11i**	**WPA2**	**WPA**	**WEP**
Utilisateur final	P	P	P	X	P	P	P	X
Commande	P	P	P	X	P	P	P	X
Gestion	X	X	X	X	X	X	X	X

Il ressort de cette analyse qu'il est possible de concevoir, de mettre en œuvre et de maintenir des WLAN relativement fiables si on utilise la norme IEEE 802.11i ou WPA2. Toutefois, la simple mise en œuvre de ces normes ne garantira pas la sécurité de bout en bout des WLAN. Comme indiqué dans cette analyse, la dimension disponibilité n'est pas prise en charge.

Bibliographie

[b-UIT-T G.729] Recommandation UIT-T G.729 (2007), *Codage de la parole à 8 kbit/s par prédiction linéaire avec excitation par séquences codées à structure algébrique conjuguée (CS-ACELP).*

[b-UIT-T X.509] Recommandation UIT-T X.509 (2005), *Technologies de l'information – Interconnexion des systèmes ouverts – L'annuaire: cadre général des certificats de clé publique et d'attribut*.

[b-UIT-T Y.2201] Recommandation UIT-T Y.2201 (2007), *Spécifications des réseaux de prochaine génération de version 1*.

[b-IETF RFC 854] IETF RFC 854 (1983), *TELNET Protocol Specification*.
<http://www.ietf.org/rfc/rfc0854.txt?number=854>

[b-IETF RFC 959] IETF RFC 959 (1985), *File Transfer Protocol (FTP)*.
<http://www.ietf.org/rfc/rfc0959.txt?number=959>

[b-IETF RFC 1321] IETF RFC 1321 (1992), *The MD5 Message-Digest Algorithm*
<http://www.ietf.org/rfc/rfc1321.txt?number=1321>.

[b-IETF RFC 1510] IETF RFC 1510 (1993), *The Kerberos Network Authentication Service (V5)*.
<http://www.ietf.org/rfc/rfc1510.txt?number=1510>

[b-IETF RFC 1661] IETF RFC 1661 (1994), *The Point-to-Point Protocol (PPP)*.
<http://www.ietf.org/rfc/rfc1661.txt?number=1661>

[b-IETF RFC 1991] IETF RFC 1991 (1996), *PGP Message Exchange Formats*.
<http://www.ietf.org/rfc/rfc1991.txt?number=1991>

[b-IETF RFC 2104] IETF RFC 2104 (1997), *HMAC: Keyed-Hashing for Message Authentication*.
<http://www.ietf.org/rfc/rfc2104.txt?number=2104>

[b-IETF RFC 2196] IETF RFC 2196 (1997), *Site Security Handbook*.
<http://www.ietf.org/rfc/rfc2196.txt?number=2196>

[b-IETF RFC 2311] IETF RFC 2311 (1998), *S/MIME Version 2 Message Specification*.
<http://www.ietf.org/rfc/rfc2311.txt?number=2311>

[b-IETF RFC 2411] IETF RFC 2411 (1998), *IP Security Document Roadmap*.
<http://www.ietf.org/rfc/rfc2411.txt?number=2411>

[b-IETF RFC 2427] IETF RFC 2427 (1998), *Multiprotocol Interconnect over Frame Relay*.
<http://www.ietf.org/rfc/rfc2427.txt?number=2427>

[b-IETF RFC 2459] IETF RFC 2459 (1999), *Internet X.509 Public Key Infrastructure Certificate and CRL Profile*.
<http://www.ietf.org/rfc/rfc2459.txt?number=2459>

[b-IETF RFC 2510] IETF RFC 2510 (1999), *Internet X.509 Public Key Infrastructure Certificate Management Protocols*.
<http://www.ietf.org/rfc/rfc2510.txt?number=2510>

[b-IETF RFC 2616] IETF RFC 2616 (1999), *Hypertext Transfer Protocol – HTTP/1.1*.
<http://www.ietf.org/rfc/rfc2616.txt?number=2616>

[b-IETF RFC 2631] IETF RFC 2631 (1999), *Diffie-Hellman Key Agreement Method*.
<http://www.ietf.org/rfc/rfc2631.txt?number=2631>

[b-IETF RFC 2661] IETF RFC 2661 (1999), *Layer Two Tunnelling Protocol "L2TP"*.
<http://www.ietf.org/rfc/rfc2661.txt?number=2661>

[b-IETF RFC 2716] IETF RFC 2716 (1999), *PPP EAP TLS Authentication Protocol*.
<http://www.ietf.org/rfc/rfc2716.txt?number=2716>

[b-IETF RFC 2748] IETF RFC 2748 (2000), *The COPS (Common Open Policy Service) Protocol*. <http://www.ietf.org/rfc/rfc2748.txt?number=2748>

[b-IETF RFC 2749] IETF RFC 2749 (2000), *COPS usage for RSVP*. <http://www.ietf.org/rfc/rfc2749.txt?number=2749>

[b-IETF RFC 2753] IETF RFC 2753 (2000), *A Framework for Policy-based Admission Control*. <http://www.ietf.org/rfc/rfc2753.txt?number=2753>

[b-IETF RFC 2828] IETF RFC 2828 (2000), *Internet Security Glossary*. <http://www.ietf.org/rfc/rfc2828.txt?number=2828>

[b-IETF RFC 2865] IETF RFC 2865 (2000), *Remote Authentication Dial In User Service (RADIUS)*. <http://www.ietf.org/rfc/rfc2865.txt?number=2865>

[b-IETF RFC 2869] IETF RFC 2869 (2000), *RADIUS Extensions*. <http://www.ietf.org/rfc/rfc2869.txt?number=2869>

[b-IETF RFC 3031] IETF RFC 3031 (2001), *Multiprotocol Label Switching Architecture*. <http://www.ietf.org/rfc/rfc3031.txt?number=3031>

[b-IETF RFC 3084] IETF RFC 3084 (2001), *COPS Usage for Policy Provisioning (COPS-PR)*. <http://www.ietf.org/rfc/rfc3084.txt?number=3084>

[b-IETF RFC 3174] IETF RFC 3174 (2001), *US Secure Hash Algorithm 1 (SHA1)*. <http://www.ietf.org/rfc/rfc3174.txt?number=3174>

[b-IETF RFC 3377] IETF RFC 3377 (2002), *Lightweight Directory Access Protocol (v3): Technical Specification*. <http://www.ietf.org/rfc/rfc3377.txt?number=3377>

[b-IETF RFC 3579] IETF RFC 3579 (2003), *RADIUS (Remote Authentication Dial In User Service) Support For Extensible Authentication Protocol (EAP)*. <http://www.ietf.org/rfc/rfc3579.txt?number=3579>

[b-IETF RFC 3580] IETF RFC 3580 (2003), *IEEE 802.1X Remote Authentication Dial In User Service (RADIUS) Usage Guidelines*. <http://www.ietf.org/rfc/rfc3580.txt?number=3580>

[b-IETF RFC 3748] IETF RFC 3748 (2004), *Extensible Authentication Protocol (EAP)*. <http://www.ietf.org/rfc/rfc3748.txt?number=3748>

[b-IETF RFC 4017] IETF RFC 4017 (2005), *Extensible Authentication Protocol (EAP) Method Requirements for Wireless LANs*. <http://www.ietf.org/rfc/rfc4017.txt?number=4017>

[b-IETF RFC 4252] IETF RFC 4252 (2006), *The Secure Shell (SSH) Authentication Protocol*. <http://www.ietf.org/rfc/rfc4252.txt?number=4252>

[b-IETF RFC 4366] IETF RFC 4366 (2006), *Transport Layer Security (TLS) Extensions*. <http://www.ietf.org/rfc/rfc4366.txt?number=4366>

[b-IETF RFC 4557] IETF RFC 4557 (2006), *Online Certificate Status Protocol (OCSP) Support for Public Key Cryptography for Initial Authentication in Kerberos (PKINIT)*. <http://www.ietf.org/rfc/rfc4557.txt?number=4557>

[b-ISO/CEI7816-x] ISO/CEI 7816-x, *Cartes d'identification – Cartes à circuit intégré*. <http://www.iso.org/iso/search.htm?qt=7816&searchSubmit=Search&sort=rel&type=simple&published=on>

[b-ISO/CEI 18028-2] ISO/CEI 18028-2:2006, *Technologies de l'information – Techniques de sécurité – Sécurité de réseaux TI – Partie 2: Architecture de sécurité de réseau*. <http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=40009>

[b-ISO/CEI 18028-3] ISO/CEI 18028-3:2005, *Technologies de l'information – Techniques de sécurité – Sécurité de réseaux TI – Partie 3: Communications de sécurité entre réseaux utilisant des portails de sécurité*.
<http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=40010>

[b-ISO/CEI 18028-5] ISO/CEI 18028-5:2006, *Technologies de l'information – Techniques de sécurité – Sécurité de réseaux TI – Partie 5: Communications sûres à travers les réseaux utilisant les réseaux privés virtuels*.
<http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=40012>

[b-ISO/CEI 18043] ISO/CEI 18043:2006, *Technologies de l'information – Techniques de sécurité – Sélection, déploiement et opérations des systèmes de détection d'intrusion*.
<http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=35394>

[b-IEEE 802.11] IEEE 802.11-2007, *IEEE Standard for Information technology – Telecommunications and information exchange between systems – Local and metropolitan area networks – Specific requirements – Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications*.
<http://standards.ieee.org/getieee802/download/802.11-2007.pdf>

[b-IEEE 802.1X] IEEE 802.1X-2004, *IEEE Standard for Local and metropolitan area networks: Port-Based Network Access Control*.
<http://www.ieee802.org/1/pages/802.1x.html>

[b-W3C XML 1.0] W3C XML 1.0 (2004), *Extensible Markup Language (XML) 1.0 (Third Edition),* W3C Recommendation, Copyright © [4 February 2004] World Wide Web Consortium, (Massachusetts Institute of Technology, Institut National de Recherche en Informatique et en Automatique, Keio University).
<http://www.w3.org/TR/REC-xml/>

[b-SSL3] The SSL Protocol Version 3.0.
<http://wp.netscape.com/eng/ssl3/draft302.txt>

[b-WPA] Wi-Fi Alliance, *Wi-Fi Protected Access*.
<http://www.wi-fi.org/white_papers/whitepaper-022705-deployingwpawpa2enterprise/>

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, 2009