DOSSIER TECHNIQUE

SECURITE ET MOBILITE

Sécurité d'accès aux systèmes d'information de l'entreprise
par le personnel hors de son lieu de travail

Commission Réseaux et Systèmes Ouverts

Juin 2002

Version 1.0

CLUB DE LA SECURITE DES SYSTEMES D'INFORMATION FRANÇAIS

30, rue Pierre Semard - 75009 PARIS

Tél. : +33 153 25 08 80 – Fax : +33 1 53 25 08 88

e-mail : clusif@clusif.asso.fr Web : http://www.clusif.asso.fr

Remerciements

Ce document a été élaboré à partir d'un draft fourni par la société Solucom. Nous tenons à remercier sa collaboration.

Nous tenons également à souligner la contribution importante des membres de la commission Réseaux et Systèmes Ouverts à la production de ce document :

BAILLEUL Emmanuel	ASCOM ADILAN
BERRANGER Laurence	THALES Systèmes Aéroportés
CHOLLET Fréderic	SOLUCOM
CONSTANT Paul	PAUL CONSTANT
CONVERSIN Philippe	6 WIND S.A
COPITET Michèle	EGONA-CONSULTING
MARCHAND Franck	MINISTERE DE LA DEFENSE
MESBAHI Rachid	FEDERATION NATIONALE MUTUALITE FRANCAISE
MUSET DUPERO Denis	SOLUCOM
PEJSACHOWICZ Lazaro	FRANCE TELECOM E-BUSINESS
RICHY Paul	FRANCE TELECOM
SCHAUER Hervé	HERVE SCHAUER CONSULTANTS

Table des matières

Liste des Tableaux

Liste des tableaux

Liste des figures

1. INTRODUCTION

1.1. OBJET DU DOCUMENT

Ce document aborde les problématiques posées par les accès aux S.I. du personnel mobile et présente des recommandations génériques pouvant être mises en œuvre.

Il met en évidence les risques présentés par ces types d'accès, selon les environnements techniques et organisationnels exploités, mais n'a pas pour objet de détailler l'ensemble des vulnérabilités encourues.

Ce document est destiné aux RSSI, Architectes de Systèmes d'Information, et toute autre personne devant effectuer des choix d'infrastructure liés à la mobilité du personnel de l'entreprise.

1.2. PERIMETRE

Ce document traite de « l'accès aux Systèmes d'information[1] du personnel de l'entreprise hors de son lieu de travail habituel » dans le périmètre déterminé ci-après.

Dans le contexte de ce document, on considère comme lieu de travail habituel l'endroit où l'employé a, à sa disposition exclusive, un équipement informatif et télécommunication parfaitement identifié et attribué de façon permanente.

1.2.1. Éléments pris en considération

Parties concernées du système d'information

La présente synthèse ne prend en considération, dans l'examen des problématiques de sécurité, que les équipements nomades, les réseaux d'interconnexion, les points d'accès au S.I. des entreprises ainsi que leur réseau interne.

En outre, elle prend pour postulat que les informations échangées ou accessibles sur le S.I. sont potentiellement sensibles vis à vis des risques d'altération ou de divulgation.

Les éléments de sécurisation présentés dans ce document seront donc systématiquement à adapter au contexte d'utilisation selon la criticité réelle des informations.

[1] Le système d'information est pris dans le sens de l'« *Ensemble de moyens matériels et logiciels assurant le stockage, le traitement et le transport (sous forme électronique) des données de l'entreprise* ».

Accès nomade et itinérant

Ce document traite spécifiquement de la sécurité des accès nomades et des accès itinérants au S.I., c'est à dire de l'accès au S.I. de l'entreprise par le personnel depuis :

- Un point du réseau de l'entreprise différent de son point de raccordement habituel (*« itinérance »*) ; bâtiment ou site différents de l'entreprise…
- Un site hors de l'entreprise (*« nomadisme »*) : hôtel, site d'un client, aéroport, domicile de la personne, s'il ne s'agit pas d'un télétravailleur.

1.2.2. Éléments hors périmètre

Système d'information

Le présent document ne prend pas en considération, dans l'analyse sécuritaire des accès nomades et itinérants :

- L'environnement physique du S.I., c'est à dire les locaux, les matériels… qui contribuent à la constitution du S.I. et sur lesquels courent principalement des risques de sinistres d'origine naturelle ou humaine.
- Les moyens humains concourant au fonctionnement du S.I. et sur lesquels peuvent peser des risques d'ingénierie sociale, d'erreurs humaines, de chantage, ….
- Les processus de gestion et d'administration du S.I., qui pourraient présenter des failles dans leur exécution ou dans leur conception, ne sont pas décrits dans leur intégralité.

En outre, les problématiques de sécurité sont examinées, de manière macroscopique, dans le cadre d'applications de type « *données* » et non de type « *voix* ». Les spécificités, en terme de sécurité, des environnements et systèmes informatiques (OS, middleware, applications, mainframes, protocoles, …) ne sont pas pris en considération.

Sécurité interne du S.I.

Le présent document ne couvre pas la sécurité interne, physique et logique, du S.I. Il prend pour postulat que le réseau d'établissement constitue un périmètre de confiance, sécurisé par des moyens techniques, humains, organisationnels et contractuels appropriés.

Utilisateurs

Seul le raccordement du personnel de l'entreprise ou du personnel externe dûment habilité à accéder au S.I. est pris en considération. Le raccordement des autres utilisateurs externes, qui soulève des problématiques de sécurité spécifiques, n'est pas examiné (clients, prestataires, partenaires, visiteurs…).

Échanges d'information non couverts

Les échanges d'information réalisés sans raccordement direct au S.I. ne sont pas pris en considération. D'autre part, ne sont pas pris en compte dans ce document :

a) l'échange direct entre deux ou plusieurs utilisateurs mobiles

b) l'échange par transfert de supports (magnétiques, optiques ou électroniques).

2. LA MOBILITE ET SON IMPACT SUR LA SECURITE DE CERTAINES FONCTIONS DU SYSTEME D'INFORMATION

Avant d'entrer dans l'analyse détaillée des failles ouvertes dans le dispositif de sécurité du SI pour permettre la prise en compte de la mobilité des personnes, nous donnons un aperçu des problèmes à aborder pour la mise en place de l'accès vers certaines fonctions du système d'information pour le personnel nomade.

Dans ce chapitre, seules quelques fonctions particulièrement importantes du point de vue du nomadisme, telles que la connexion à une application, le courrier électronique et la protection des données, seront abordées. Nous croyons que les RSSI et Responsables du Système d'Information pourront s'inspirer de la démarche analytique utilisée pour l'appliquer à d'autres situations similaires.

2.1. DEFINITION

L'équipement terminal est l'équipement dont dispose le personnel mobile pour effectuer ses opérations d'interrogation, de consultation et / ou de modification des données du système d'information de l'entreprise. Trois familles d'équipements apparaissent :

- Les postes de travail (postes informatiques)
- Les assistants personnels numériques (PDA)
- Les téléphones mobiles évolués (téléphones WAP)

Postes informatiques

Nous désignons par poste informatique un poste de travail, portable ou fixe, constitué, sous l'angle de la sécurité, des éléments suivants :

- Un espace de stockage des données (mémoire, disque dur, …) et des applications
- Un système d'exploitation comportant des couches de communication
- Un ou plusieurs sous-systèmes de communication (modem, Ethernet, …)

Deux catégories de postes informatiques se distinguent :

- Les postes « maîtrisés » par l'entreprise.

Le poste informatique est dit maîtrisé par l'entreprise lorsqu'il est configuré, sécurisé et mis à disposition par ses soins, à un employé nomade qu'elle engage à ne pas en modifier la configuration.

- Les postes non « maîtrisés ».

Par opposition, il s'agit de poste, portable ou fixe, ni configuré et ni sécurisé par l'entreprise ; postes chez un partenaire ou client, postes personnels (à domicile), postes d'un hôtel ou d'un web café.

Assistant personnel numérique (PDA)

Un PDA (assistant personnel numérique) est un petit ordinateur de poche, principalement destiné à l'amélioration de la productivité personnelle ; gestion des contacts et de l'agenda, liste des tâches à faire, calculatrice. Les deux familles les plus représentées sur le marché s'appuient respectivement sur les systèmes d'exploitation PalmOS et WinCE / PocketPC.

Un PDA a la capacité d'héberger des applications client/serveur et des navigateurs (WAP, HTTP). Il intègre, en outre, des moyens matériels et logiciels de raccordement à d'autres équipements informatiques (câble série et infrarouge) ainsi qu'à des réseaux de données (TCP / IP, Bluetooth, 802.11b, modem, …).

Deux modes de raccordement sont proposés par les PDA :

- Mode asynchrone, au moyen de logiciels de type client / serveur

Il repose sur un mécanisme de synchronisation par lequel les données sont reproduites sur le PDA et le S.I, en fonction des modifications effectuées.

- Mode synchrone, au moyen d'un navigateur léger (type WAP ou HTML)

Dans ce mode connecté, la consultation et la modification des données s'effectuent en ligne directement sur le serveur. Compte tenu des faibles débits de raccordement (9,6kbps : GSM / 35 à 40kbps : GPRS), ce mode reste encore peu employé.

Enfin, deux catégories de PDA peuvent être distinguées selon que les PDA sont « *maîtrisés* » ou non par l'entreprise (cf. définition des postes informatiques).

Téléphone mobile WAP

Il s'agit d'un téléphone sans fil fonctionnant sur l'un des trois réseaux numériques GSM, GPRS, ou UMTS et doté d'un navigateur léger WAP et des couches de communication associées (protocoles WDP, WTLS, WTP, WSP).

2.2. MOBILITE ET DROITS LIES A L'ADRESSE RESEAU

Il est assez fréquent de trouver dans les SI des entreprises des droits d'accès aux informations et ressources liées à l'adresse IP de la station connectée. Au niveau du LAN d'un site, cette adresse est en effet censée représenter un utilisateur, même si, comme nous le savons, la substitution n'est pas bien difficile pour un pirate d'un niveau technique moyen.

Mais nous pouvons considérer que, en complément à d'autre type d'identifiant, cette technique ajoute une barrière supplémentaire.

Or, la mobilité de l'employé fait perdre ce contrôle d'adresse avec, comme conséquence, la difficulté de restituer ses droits à l'utilisateur. Les solutions sécurisées pour la restitution de ces droits vont dépendre de l'endroit où se trouve l'utilisateur et de l'équipement utilisé.

Dans ce que suit, l'analyse est faite pour l'utilisation d'une station de type PC, mais des analyses similaires peuvent être faites pour les autres équipements. De plus, le changement d'adresse IP du PC en forme statique revient à traiter un nouveau micro en position fixe. Nous ne traiterons donc que les réseaux utilisant DHCP pour la gestion de la mobilité.

2.2.1. Mobilité de l'employé avec un poste « maîtrisé »

a) Connexion à partir d'une autre prise du même LAN.

Il n'y a de perte d'adresse que s'il y a changement de sous-réseau du point de vue du DHCP. Dans ce cas, la situation est identique à un changement de site.

b) Connexion à partir d'un autre site de la même entreprise.

Normalement, à la connexion, le PC reçoit une nouvelle adresse IP « à la volée » Cette adresse étant « impersonnelle » des mesures d'authentification complémentaires (VPN, mot de passe Windows, etc.) sont nécessaires pour donner des droits précis à un utilisateur.

c) Connexion à partir de son domicile, hôtel ou autres par RTC.

Tout d'abord, il n'est ni nécessaire ni conseillé d'attribuer de façon générale les mêmes droits d'accès à un employé se trouvant hors des locaux de sa société que ceux qu'il a quand il se trouve à son travail (sauf cas de télétravail). Habituellement, les systèmes de connexion à distance vont travailler avec l'attribution d'une adresse dynamique par DHCP. On se trouve donc dans la même situation que le point précédant mais, étant donné le manque de confidentialité de la connexion (PPP sur RTC), le VPN est largement conseillé.

d) Connexion à partir de son domicile, hôtel ou autres par Internet.

Ces connexions, de plus en plus utilisées, sont les plus fragiles du point de vue de la sécurité en raison du nombre important de scénarios de risque. C'est la raison qui a conduit beaucoup d'entreprises à construire des portails spécifiques d'accès aux systèmes d'information de l'entreprise. Ceci permet de palier à l'absence d'une identification de l'adresse IP qui dans ce cas est propre au FAI utilisé et hors du contrôle de l'entreprise. De plus, puisque l'employé conserve son équipement, cela permet d'utiliser des protocoles sécurisés mettant en jeu des mécanismes de sécurité plus forts (certificat utilisateur couplé ou non à une carte à mémoire, clé USB, token ou calculettes physiques, etc.) Comme dans le cas précédent, l'utilisation d'un chiffrement de type VPN non seulement renforce l'identification mais offre aussi la confidentialité aux services qui seront utilisés pendant la session et qui ne sont pas protégés dans ce domaine (FTP, Mail, etc.).

2.2.2. Mobilité de l'employé utilisant un poste « non-maîtrisé »

Tout d'abord, nous attirons l'attention du lecteur sur les risques intrinsèques à l'utilisation d'un poste « non-maîtrisé ». Ce risque est donné, d'un côté, par des éléments pouvant être présents sur l'équipement (virus, Chevaux de Troie, logiciels illisibles, etc.) et de l'autre, par des traces pouvant être retrouvées par le propriétaire de l'équipement après l'utilisation de celui-ci.

a) Connexion à partir d'une autre prise du même LAN ou connexion à partir d'un autre site.

L'équipement n'appartenant pas à l'utilisateur il n'est pas possible d'utiliser l'adresse IP comme identifiant. Il faut donc s'appuyer sur des identifications complémentaires dont la première et la plus simple est le login dans un domaine Windows si celui-ci est défini et géré.

b) Connexion à partir de son domicile, hôtel ou autres par RTC.

Même si l'utilisateur doit réaliser un travail fastidieux de configuration (et porter sur lui les paramètres du service) il est possible de configurer l'accès distant de la même façon que celui-ci est configuré sur le poste portable des utilisateurs. Mais attention : les utilisateurs ont tendance à laisser les paramètres sur le poste y compris le mot de passe de la connexion. Il est donc préférable, dans la mesure du possible de leur déconseiller d'utiliser des connexions Internet sur des postes « non-maîtrisés ».

c) Connexion à partir de son domicile, hôtel ou autres par Internet.

Au premier abord, nous pourrions dire que cette situation peut être traitée de la même façon que la connexion par Internet à partir de son propre portable. Pourtant, nous devons faire attention à tout mécanisme basé sur une installation logiciel sur le PC, qui risquerait de rester sur l'équipement comme dans le cas précédent. Ceci est particulièrement vrai pour les « certificats X509 », qui doivent être recopiés sur le disque pour être supportés par les browsers. Il est donc préférable d'utiliser des éléments matériels externes et portables tel que les calculettes ou les cartes à mémoire en format « clé USB ». La connexion Internet depuis un hôtel peut présenter des risques particuliers dus au manque total de maîtrise de la connexion. On ne maîtrise pas quels équipements on traverse ni quel type d'enregistrement peut avoir sur ces équipements.

2.3. MOBILITE ET ACCES AU COURRIER ELECTRONIQUE

L'établissement des connexions et des canaux sécurisés, autant du point de vue de l'identification que de la confidentialité de la connexion, sont des solutions globales au problème de l'accès à la messagerie du personnel mobile. Nous constatons que très fréquemment cet accès est le seul besoin de ce personnel. Il est intéressant de passer en revue les problèmes rencontrés du point de vue de la sécurité, ainsi que les solutions pouvant être mises en œuvre, solutions moins solides que le VPN, mais aussi beaucoup moins chères.

Un premier constat est que le protocole POP3, le plus populaire des protocoles régissant les échanges entre le serveur de messagerie et le client sur le poste de travail, reste largement utilisé non seulement dans les offres de messageries personnelles des différents FAI mais aussi dans de très nombreuses entreprises et, en particulier, pour donner accès au personnel hors leur réseau d'entreprise.

Or ce protocole présente de nombreux inconvénients :

a. L'identification est faible : l'identifiant et le mot de passe sont transmis en clair.

b. Le texte des messages est transmis en clair.

c. Du point de vue de la disponibilité, la transmission de l'ensemble des messages sans possibilité d'arrêt ni reprise est un point de faiblesse évident, surtout si le support de communication n'est pas fiable.

d. C'est, de loin, le protocole le plus attaqué.

Par contre, si ce protocole reste le plus utilisé, c'est par son support par tous les clients de messagerie (« User Agent ») et la facilité de configuration sur un poste. De plus, il présente un certain nombre d'avantages pour la gestion de l'espace de stockage puisqu'il est « naturel » de retirer l'ensemble des messages du serveur.

2.3.1. L'accès à la messagerie depuis un point du réseau de l'entreprise

Aucun des systèmes et protocoles de messagerie ne pose de difficulté majeure pour la mobilité dans l'entreprise à condition d'utiliser son poste. Celui-ci contient les paramètres de connexion et, dans certains cas le certificat de l'utilisateur. Les serveurs sont en général centralisés et pour les entreprises disposant d'un réseau interne, accessibles de tous les sites.

Pourtant, il faut faire attention aux faiblesses du protocole POP3 : son système d'identification très simplifié et la fonction d'enregistrement de mot de passe standard sur la plupart des clients font que le « sport » de prélever des messages sur la BAL d'un autre utilisateur est assez simple à pratiquer. Ce détournement d'informations est encore plus simple si le pirate peut accéder aux traces d'un élément de communication entre le client et le serveur (trace sur routeur par exemple).

Pour cette raison il est préférable d'utiliser en interne des protocoles de messagerie plus évolués tel que MAPI ou IMAP4 offrant des possibilités de renforcer l'identification mais aussi de consulter les entêtes des messages sans les retirer. Par ailleurs des solutions de type Webmail - abordées dans le § 2.2.3 – et conseillées pour la mobilité externe, sont aussi utilisables sur le réseau interne. Cependant, elles offrent une interface assez inconfortable.

2.3.2. L'accès à la messagerie depuis son domicile, hôtel ou tout autre lieu avec un poste « maîtrisé »

Une solution assez évidente est de réduire le problème à la sécurisation de la connexion telle que nous l'avons développée dans le chapitre précédent.

Dans le cas d'une connexion par RTC et même sans le chiffrement de la transmission, l'utilisation du POP3 est acceptable. Ceci parce qu'il y a eu au préalable une connexion réseau et que l'écoute des lignes RTC n'est pas une technique de piratage usuelle.

L'ouverture de la messagerie sur Internet, permettant l'accès du client messagerie vers le serveur est particulièrement dangereuse, non seulement parce qu'on peut attaquer les BALs des utilisateurs mais aussi en raison de l'ouverture du relais SMTP.

En effet, pour que l'utilisateur puisse non seulement recevoir les messages mais aussi les envoyer, il faut permettre au client de se relayer sur le port 25 (SMTP) du serveur ce qui met l'entreprise face au risque de servir de relais aux « spams » (messages non désirés) et de faire l'objet d'une mise en liste noire voire d'un procès aux Etats Unis. Nous en profitons pour rappeler que le filtrage des domaines relayés est une obligation sur la messagerie.

Il est possible d'utiliser les mêmes solutions que dans le cas d'un équipement étranger que nous développerons ci-dessous.

2.3.3. L'accès à la messagerie depuis son domicile, hôtel ou tout autre lieu par poste « non-maîtrisé »

L'accès par RTC, dans ce cas, est possible mais pas pratique. Il faut configurer et récupérer le message à l'identique de ce qu'on ferait avec son propre poste, avec les possibilités d'oubli des paramètres (mot de passe compris) et / ou des messages sur le poste utilisé.

Dans le cas d'un accès par Internet, il existe une solution simple et efficace à condition de la mettre en œuvre dans son système de messagerie : il s'agit du Webmail qui est une interface d'accès par http à ses boîtes aux lettres.

Le Webmail est un logiciel d'intermédiation qui, après avoir demandé la saisie de l'identifiant et du mot de passe, permet d'accéder à la liste des messages et à la lecture de chaque message, qui restent en principe sur le serveur. L'avantage de ce système est de pouvoir utiliser la protection normale d'un Web, c'est à dire de protéger les informations (identifiant et mot de passe inclus) par l'utilisation du protocole SSL avec le certificat du serveur.

Ce système utilisant le protocole http il évite l'ouverture d'autres ports sur le «pare-feu» d'accès au Système d'Information.

Par contre le Webmail est peu pratique pour une utilisation intensive, surtout si l'utilisateur veut sauvegarder ses messages sur son poste. Dans ce cas, il faut plutôt prévoir l'utilisation d'un autre protocole quand l'utilisateur est à son bureau.

De plus, les utilisateurs ne faisant pas d'attention particulière au poste utilisé pour accéder au Webmail, il est impératif d'avoir un logiciel anti-virus actif et à jour sur le serveur Webmail, pour le traitement de pièces jointes.

Pour conclure ce chapitre, disons tout le mal que nous pensons des systèmes de « renvoi vers une autre boîte » comme moyen de transmettre des messages d'un utilisateur hors entreprise vers une autre messagerie facilement accessible par l'utilisateur, tel sa propre messagerie ou encore des BALs accessibles par Webmail offertes « gratuitement » par beaucoup de FAI et certaines entreprises. Ce système est la porte ouverte à la sortie de l'information sensible de l'entreprise vers des endroits complètement déprotégés. Et, hélas, dans le cas général, il est difficile à éviter techniquement, surtout si le PC «client» de l'utilisateur reste dans son bureau. Ce type d'utilisation doit être proscrit par la Charte Informatique voir par le Règlement Intérieur de l'entreprise[2].

2.4. MOBILITE ET PROTECTION DES DONNEES

La protection des informations acquises ou manipulées par une personne travaillant à l'extérieur de son entreprise est aussi une préoccupation importante pour le Directeur Informatique et le Responsable de la Sécurité du Système d'Information.

Tout d'abord, il faut protéger les informations sur les stations de travail mobiles, c'est à dire mettre en œuvre des mécanismes de chiffrement efficaces et simples d'utilisation. Il en existe une grande variété. Windows 2000 offre, en plus, des possibilités de chiffrement des données en standard. Bien sur, cette mise en place doit être accompagnée d'une politique de sensibilisation des utilisateurs sur la qualité des mots de passe à utiliser et le non-enregistrement du mot de passe sur la station. Un « token » physique d'accès à la station est un atout de protection complémentaire, nécessaire dans certains cas.

Mais il ne suffit pas de protéger la confidentialité des données.

La mobilité augmente la « fragilité » de la station de travail et le risque de perdre les données saisies ou acquises. Il faut donc permettre à l'utilisateur de sauvegarder facilement les données les plus importantes. Or, s'il est relativement facile de mettre en place un système de sauvegarde des données, ces systèmes sont trop gourmands au niveau du réseau pour être utilisés sur des accès distants ou par Internet. Il est donc préférable de fournir à l'utilisateur qui bouge avec son portable des moyens de sauvegarde locale, tels un lecteur Zip ou un équipement ayant un graveur de CD.

[2] Voir le document « Guide d'élaboration d'une charte d'utilisation des moyens Intranet et Internet », éditée par le CLUSIF en mai 2002.

Cette sauvegarde n'est que provisoire. Pour des questions de cohérence il est largement conseillé que le collaborateur, une fois rentré sur sa « base », sauvegarde ses informations sur un serveur centralisé.

Mais ceci implique la prise en compte de la mobilité dans les systèmes de sauvegarde des PC. Et le travail est particulièrement délicat s'il s'agit de mettre en place un système de sauvegarde automatique déclenché par le serveur de sauvegarde.

3. CHAINE DE LIAISON DE L'ACCES NOMADE AU S.I.

3.1. MODELE DE CHAINE DE LIAISON

Afin d'aborder les problématiques de sécurité posées par la mobilité du personnel, nous examinons la chaîne de liaison type caractérisant un accès nomade (ou itinérant) et assurant l'interconnexion d'un utilisateur mobile à son S.I.

Cette chaîne de liaison type est modélisée au moyen de cinq éléments génériques (cf. figure ci-dessous) pour lesquels sont réalisés, dans les chapitres suivants, une rapide analyse des risques en matière de sécurité logique et un bref examen des parades qui leur sont potentiellement opposées.

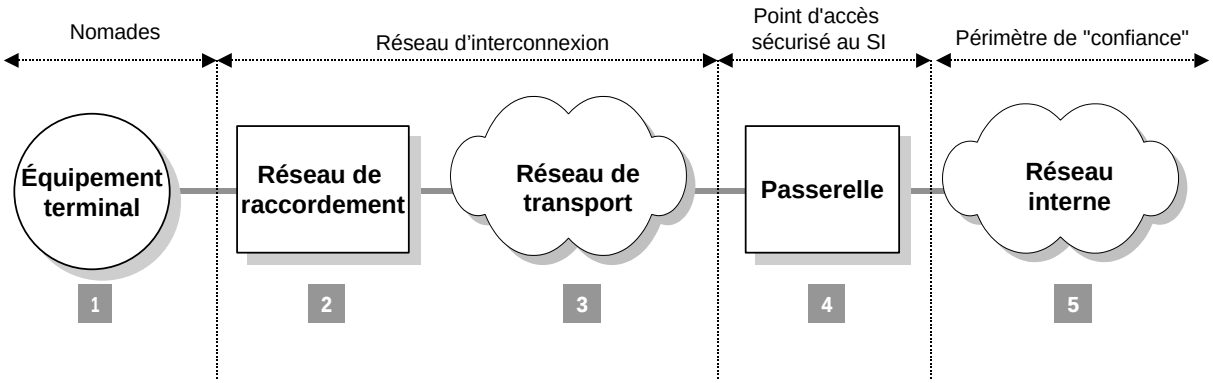

Figure 1 : Modèle de la chaîne de liaison

Certaines natures d'éléments (assistant personnel, technologie de transmission sans fil Bluetooth, 802.11b…) sont examinées plus avant, compte tenu de leurs caractères « *nomade* » et novateur.

3.2. ÉQUIPEMENT TERMINAL

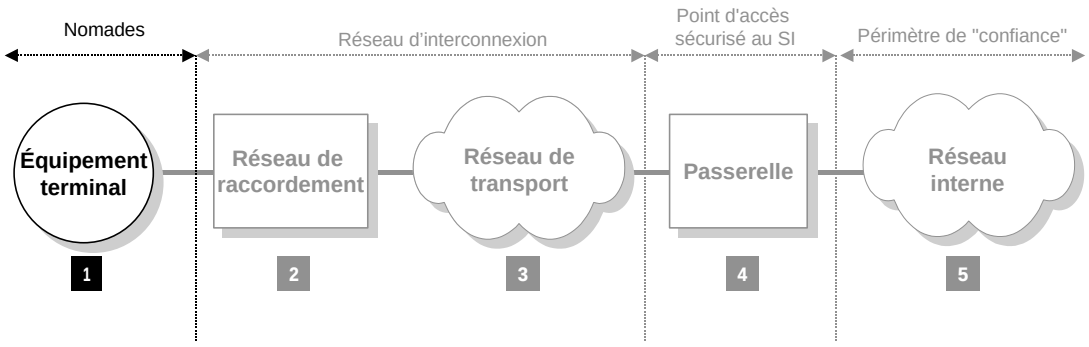

Figure 2 : Équipement terminal

3.2.1. Problématiques de sécurité

Menaces pesant sur l'équipement terminal

L'équipement terminal constitue un des maillons faibles de la chaîne de liaison de par ses caractéristiques :

- Sa mobilité accroît les risques de vol, de détérioration et de divulgation.
- La multiplicité des moyens de raccordement (Ethernet, ondes radio, modem, …) et la potentialité de leur simultanéité augmente les risques d'accès ou d'écoute illicites et de rebond.
- Ses capacités de stockage (conservation d'informations issues du S.I. de l'entreprise ou produites par l'utilisateur) accroissent l'impact d'un vol ou d'accès illicites.
- Son caractère potentiellement multi-utilisateurs (partage au sein de l'entreprise) augmente la probabilité d'altération ou de divulgation des données.

N°	Menaces	Impacts			
		D	I	C	Poids
Men.1.	Vol ou perte de l'équipement	✓		✓	2
Men.2.	Défaillance technique de l'équipement *Panne matérielle / Saturation matérielle ou logicielle / Dysfonctionnement matériel ou logiciel*	✓			3
Men.3.	Détérioration, destruction physique de l'équipement	✓			2
Men.4.	Altération ou perte des données *Virus, vers, cheval de Troie / Erreur de saisie ou d'utilisation*	✓	✓	✓	3
Men.5.	Accès illicites *Utilisation illicite, abusive / Usurpation, abus des droits*		✓	✓	2
Men.6.	Déni de service	✓	✓		2
Men.7.	Divulgation d'information			✓	2

Tableau 1 : Menaces génériques pesant sur l'équipement terminal

La pondération signifie :

2) Potentialité d'occurrence moyenne : si ses conséquences sont redoutées, certaines parades peuvent s'avérer utiles pour s'en prémunir.

3) Potentialité d'occurrence haute : si ses conséquences sont redoutées, il est indispensable de mettre en œuvre les parades pour s'en prémunir.

La menace se réalise fréquemment : si ses conséquences sont redoutées, il est indispensable de mettre en œuvre les parades pour s'en prémunir.

Vulnérabilités

Vulnérabilités génériques

L'équipement terminal présente un certain nombre de faiblesses ou de failles génériques liées à sa conception, à son fonctionnement ou ses modes d'utilisation :

N°	Vulnérabilités
Vul.1.	Fiabilité de l'équipement ou de ses composants *Fragilité (mécanique, électrique, électronique) / obsolescence / défaut de maintenance*
Vul.2.	Équipement attractif (valeur vénale, valeur technologique, mobilité, …) mal protégé
Vul.3.	Équipement disposant d'un ou de plusieurs modes de raccordement
Vul.4.	Possibilité de consulter, modifier, supprimer les paramètres de connexion au S.I.
Vul.5.	Défauts, failles dans la conception ou l'implémentation de l'équipement (OS, applications)
Vul.6.	Complexité d'utilisation, manque d'ergonomie de l'équipement et de ses applications
Vul.7.	Caractère multi-utilisateurs de l'équipement

Tableau 2 : Vulnérabilités génériques des équipements terminaux

Vulnérabilités propres aux postes informatiques

Les postes informatiques, qui constituent les équipements terminaux les plus complexes (en termes de capacité de stockage, de connectivité, d'applications, …), présentent également des vulnérabilités plus nombreuses que pour tout autre type d'équipement terminal.

N°	Vulnérabilités
Vul.8.	Possibilité d'infecter les applications de l'équipement
Vul.9.	Possibilité d'ajouter des composants matériels additionnels
Vul.10.	Possibilité d'installer, modifier ou supprimer des applications
Vul.11.	Possibilité de mal configurer ou mal installer des applications
Vul.12.	Possibilité de consulter, modifier, supprimer les informations
Vul.13.	Possibilité d'exploiter certaines commandes du système d'exploitation

Tableau 3 : Vulnérabilités affectant les postes de travail

Pour les postes « maîtrisés » par l'entreprise, certaines vulnérabilités peuvent être amoindries voire supprimées. En revanche, la potentialité de ces vulnérabilités est forte dans le cas de postes non maîtrisés (postes personnel, à domicile, chez un client ou partenaire, …).

Vulnérabilités propres aux PDA

Le PDA offre la possibilité de manipuler et de conserver localement des données (agenda électronique, répertoire téléphonique, documents bureautiques) mais également d'interagir avec le S.I.

Outre les vulnérabilités génériques évoquées pour les équipements terminaux, le PDA se voit également affecté par certaines vulnérabilités des postes de travail.

N°	Vulnérabilités
Vul.14.	Possibilité d'infecter les applications
Vul.15.	Possibilité d'installer, modifier ou supprimer des applications
Vul.16.	Possibilité de consulter, modifier, supprimer les informations
Vul.17.	Possibilité d'exploiter certaines commandes du système d'exploitation *Suppression du mot de passe sur le PalmOS*
Vul.18.	Possibilité d'affecter ou d'exploiter le processus de synchronisation
Vul.19.	Conservation en clair du mot de passe d'accès au PDA (PalmOS)
Vul.20.	Faiblesse des algorithmes de chiffrement (PalmOS)

Tableau 4 : Vulnérabilités affectant les PDA

Vulnérabilités propres aux téléphones WAP

Les données conservées sur les téléphones WAP consistent, pour l'essentiel, aux informations du répertoire téléphonique (de la carte SIM et de la mémoire du portable). Le protocole WAP s'appuie, pour sa part, sur un mode de connexion synchrone. Ainsi, les informations sont consultées, saisies ou modifiées, sur le serveur WAP cible, sans conservation locale, limitant la portée des attaques.

Par ailleurs, le protocole WAP intègre une couche de sécurité appelée WTLS (*Wireless Transaction Layer Security*) [3] qui s'inspire, dans les grandes lignes, des principes de fonctionnement des protocoles SSL 3.0 et TLS 1.0. Toutefois, son utilisation n'est pas systématiquement requise par les serveurs WAP.

En outre, compte tenu de la bande passante faible et des temps de latence important qui caractérisent les connexions téléphoniques mobiles, des optimisations ont été appliquées sur la taille des paquets et la négociation des clefs.

Enfin, l'authentification des parties (assurée avant l'établissement du tunnel chiffré à l'aide de certificats) n'est obligatoire, pour le client et pour le serveur, qu'à partir des spécifications WAP 1.2[3].

En raison des concessions consenties pour assurer l'adaptation de SSL au monde mobile (optimisations, authentification partielle, …), les protocoles WAP/WTLS comportent un certain nombre de failles et faiblesses [4].

Ainsi, le mode datagramme supporté par WTLS se prête davantage à la modification des paquets. En outre, WTLS tolère des algorithmes de chiffrement moins consommateurs de ressources, mais également moins robustes. La même clef secrète peut être utilisée pendant une période de plusieurs jours. Le passage par une passerelle WAP induit une conversion de protocole (WTLS vers SSL / TLS) qui entraîne une rupture de la chaîne de sécurité.

[3] Les spécifications WAP 1.2 ne sont mises en œuvre que sur les téléphones WAP les plus récents.

Enfin, certaines précautions d'implémentation sont nécessaires. L'authentification du serveur n'est pas, par exemple, automatique.

N°	Vulnérabilités
Vul.21.	Possibilité de consulter, modifier, supprimer les entrées du répertoire
Vul.22.	Identification de l'utilisateur par son numéro de téléphone
Vul.23.	Possibilité de ne pas réclamer l'authentification du serveur sur WTLS
Vul.24.	La conversion de WTLS vers SSL / TLS induit une rupture de la chaîne de sécurité

Tableau 5 :Vulnérabilités affectant les téléphones WAP

3.2.2. Éléments à sécuriser et parades éventuelles

Postes informatiques

Les postes informatiques – équipements terminaux les plus répandus – constituent la cible la plus fréquente des malveillances. En outre, leur architecture technique plus complexe (présence de pièces mécaniques) accroît la probabilité de pannes.

Pour les postes informatiques « maîtrisés » par l'entreprise, une politique de sécurisation physique et logique doit donc être mise en œuvre afin d'amoindrir la probabilité d'occurrence des risques encourus par les postes et leur contenu.

N°	Parades
Par.1.	Protection physique *tatouage, câble, cadenas, …*
Par.2.	Restriction d'accès au poste *mots de passe au démarrage du poste (BIOS) et après une période d'inactivité,* *cartes à puces, cartes de protection locale, clefs USB, mécanismes biométriques*
Par.3.	Protection du poste et de son contenu *antivirus et firewall locaux, chiffrement des informations sur disque*
Par.4.	Verrouillage du poste *protection du compte administrateur local,* *désactivation de la connexion par modem lors d'une connexion au réseau d'établissement*
Par.5.	Sauvegarde régulière des données du poste

Tableau 6 : Parades relatives aux postes de travail maîtrisés

Les postes informatiques « *non maîtrisés* » par l'entreprise (postes chez un client, un fournisseur, au domicile, à l'hôtel, …) ne sont pas, par définition, sécurisés par l'entreprise. Leur propriétaire est seul responsable de l'application de mécanismes de sécurité. En conséquence ces postes ne peuvent être considérés de confiance et aucune information ne doit y être conservée.

N°	Parades
Par.6.	Procédures d'usage *Définissant les règles de bon usage de moyen informatique non maîtrisé (pas de sauvegarde locale des mots de passe, des données de l'entreprise…)*
Par.7.	Restriction d'utilisation aux seuls flux web HTTPS supportés par tout navigateur
Par.8.	Recours à une authentification forte par jeton *(SecurID, ActiveCard…)*

Tableau 7 : Parades relatives aux postes de travail non maîtrisés

PDA

Les assistants personnels numériques ne constituent pas encore la cible privilégiée des pirates. Toutefois, plusieurs failles ont déjà été recensées [1] et des attaques virales ont été identifiées, notamment concernant les deux familles de produits PalmOS et PocketPC. Nous pouvons citer, pour le PalmOS, les exemples suivants :

- Conservation en clair du mot de passe.
- Chiffrement aisément cassable du mot de passe lors de la synchronisation.
- Suppression du mot de passe par simple appel à une fonction système.
- Porte dérobée permettant la récupération des bases en mode déboguage.
- Conservation des bases sur le poste informatique, sans chiffrement permettant la consultation des enregistrements personnels.
- Code malveillant Liberty.A, Phase.A et Vapor.A.

La vulnérabilité la plus importante réside, en cas de vol, dans les données embarquées sur le PDA. La parade la plus efficace consiste à opter pour une consultation en ligne des données afin d'éviter le processus de synchronisation (i.e. la réplication locale des informations).

N°	Parades
Par.9.	Protection du PDA et de son contenu *Chiffrement des données sensibles (PDABomb,RSA Wireless Security…)* *Verrouillage par mot de passe à l'arrêt / redémarrage du PDA (EasyLock, OnlyMe…)* *Bases de données protégées et chiffrées (eWallet…)* *Antivirus local (for wireless)*
Par.10.	Amélioration du processus de synchronisation *Plate-forme de synchronisation assurant l'authentification (y compris forte), la mise à jour des applications installées, la sauvegarde et le contrôle de configuration pouvant alerter en central en cas d'anomalies*
Par.11.	Recours à des applications en mode connecté (sur client léger) *Lors des conceptions d'applications internes, privilégier les applications en mode connecté (sur client WAP ou navigateur HTML) aux applications client/serveur (synchronisation)*

Tableau 8 : Parades relatives aux PDA

Téléphones WAP

Par construction, les téléphones WAP ne permettent pas l'adjonction de mécanismes de sécurité pouvant pallier les risques identifiés. Il convient donc de s'assurer de l'intégration des spécifications les plus récentes (WAP 1.2) dans les téléphones au moment de leur acquisition.

La vulnérabilité due à l'authentification de l'utilisateur sur le numéro de téléphone portable peut être contournée par la demande de fourniture d'un secret à l'utilisateur.

N°	Parade
Par.12.	Authentification de l'utilisateur sur la fourniture d'un secret non conservé par le téléphone *Afin d'éviter l'authentification sur le numéro de téléphone*
Par.13.	Activation de l'authentification du client et du serveur sur la passerelle WAP
Par.14.	Ouverture d'une connexion sécurisée WTLS avec négociation systématique d'algorithmes de chiffrement les plus robustes

Tableau 9 : Parades relatives aux téléphones WAP

3.3. RESEAU D'INTERCONNEXION

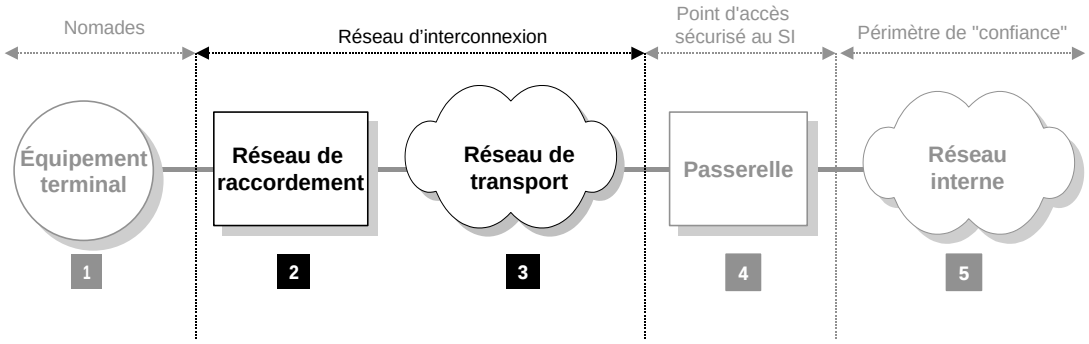

Figure 3 : Réseau d'interconnexion

3.3.1. Définition

Le réseau d'interconnexion permet le raccordement de l'équipement terminal au point d'accès sécurisé de l'entreprise. Il est constitué, fonctionnellement :

- D'un réseau de raccordement

  Le réseau de raccordement constitue le point d'accès physique de l'équipement terminal à l'infrastructure d'interconnexion. Il englobe le système de communication présent sur l'équipement terminal, un média physique et le premier système de communication présent chez l'opérateur ou l'entreprise. Quatre modes de raccordement sont distingués :

- Liaisons permanentes physiques ou logiques. Elles couvrent les liaisons louées, les liaisons Frame Relay, …, ainsi que les raccordements de type ADSL et modem câble.
- Réseaux téléphoniques commutés, analogique (RTC) et numérique (RNIS)
- Téléphonie mobile (GSM, GPRS, UMTS)
- Connexions sans fil (Bluetooth, IEEE 802.11)

- D'un réseau de transport

  Le réseau de transport est le support au transport des données échangées entre l'équipement terminal et le point d'accès au S.I. de l'entreprise. Il est constitué d'une infrastructure d'interconnexion bâtie sur un ou plusieurs réseaux opérateurs ;

  - Réseau opérateur(s) : RTC, RNIS, Frame Relay, ATM, IP…
  - Partie du réseau du ou des opérateurs affectée de manière logique à l'entreprise. L'infrastructure peut être mutualisée physiquement entre différents clients, mais son étanchéité est assurée et garantie par le ou les opérateurs.
  - Réseau Internet : ensemble des réseaux IP interconnectés d'opérateurs, d'entreprises, d'administrations, etc., assurant à chacun la visibilité de l'ensemble des nœuds d'Internet.

3.3.2. Problématiques de sécurité

Menaces pesant sur le réseau d'interconnexion

Les menaces citées ci-après concernent conjointement le réseau de raccordement et le réseau de transport.

N°	Menaces	Impacts			Poids
		D	I	C	
Men.1.	Défaillance technique d'un équipement du réseau *Panne matérielle / dysfonctionnement matériel ou logiciel*	✓			2
Men.2.	Détérioration physique d'équipements du réseau	✓			1
Men.3.	Vol de matériel	✓			1
Men.4.	Écoutes illicites *Copie d'informations métiers, des séquences d'authentification…*			✓	2
Men.5.	Altérations des informations en transit *Modification, insertion dans les connexions en cours…*		✓	✓	1
Men.6.	Rebond *Sur les équipements présents sur le réseau ou aux extrémités (équipement terminal, passerelle d'accès au S.I.)*	✓			1
Men.7.	Prise de contrôle d'équipement	✓			1
Men.8.	Déni de service *Saturation matérielle ou logicielle / exploitation de failles*	✓			3
Men.9.	Fraude *Non facturation / utilisation abusive du réseau*	✓			1

Tableau 10 : Menaces génériques pesant sur le réseau d'interconnexion

La pondération signifie :

1) Potentialité d'occurrence faible : la menace ne constitue pas un réel danger.

2) Potentialité d'occurrence moyenne : si ses conséquences sont redoutées, certaines parades peuvent s'avérer utiles pour s'en prémunir.

3) Potentialité d'occurrence haute : si ses conséquences sont redoutées, il est indispensable de mettre en œuvre les parades pour s'en prémunir.

Vulnérabilités

Vulnérabilités génériques du réseau d'interconnexion

Les faiblesses et failles du réseau d'interconnexion tiennent à ses éléments constitutifs (équipements et médias physiques ; *fibre optique*, *câble en cuivre*, *ondes radioélectriques*, …), leur administration et leur exploitation (installation, configuration, maintenance).

N°	Vulnérabilités
Vul.1.	Fiabilité des équipements constituant le réseau *Fragilité (mécanique, électrique, électronique) / obsolescence / défaut de maintenance*
Vul.2.	Matériel attractif (valeurs vénales, technologique, stratégique, encombrement réduit)
Vul.3.	Caractéristiques techniques permettant ou facilitant l'écoute
Vul.4.	Possibilité d'erreur dans l'installation ou la configuration des équipements
Vul.5.	Défauts, failles dans la conception ou l'implémentation des équipements
Vul.6.	Le réseau peut être détruit ou perturbé *Ondes électromagnétiques, travaux publics…*

Tableau 11 : Vulnérabilités affectant le réseau d'interconnexion

Vulnérabilités propres aux réseaux commutés

N°	Vulnérabilités
Vul.7.	Possibilité de raccordement illicite au point d'extrémité du réseau commuté. *Les points d'extrémité des réseaux commutés sont généralement situés sur la voie publique sans protection.*

Tableau 12 : Vulnérabilités affectant les réseaux commutés

Vulnérabilités propres aux liaisons permanentes

Les liaisons permanentes peuvent être séparées en deux familles :

- Liaison physique (ADSL, modem câble) sur le domaine public (rue, maison, immeuble).
- Liaison site à site d'une entreprise, physique ou logique.

Dans le premier cas, la potentialité d'une écoute illicite est plus importante compte tenu du raccordement physique chez l'abonné (non protégé) et de la nature de la liaison (paire de cuivre ou liaison coaxiale).

Dans le second cas, les arrivées de liaison aboutissent dans des locaux techniques de l'entreprise dont l'accès peut être contrôlé et restreint, ce qui diminue la potentialité d'une écoute illicite. Cette potentialité est réduite par le recours à des médias protégés (fibre optique) ou des liaisons logiques sur le réseau d'un opérateur.

N°	Vulnérabilités
Vul.8.	Possibilité de raccordement illicite au point d'extrémité de la liaison permanente.
Vul.9.	Possibilité de raccordement illicite sur la liaison physique *paire de cuivre, liaison coaxiale,...*

Tableau 13 : Vulnérabilités affectant les liaisons permanentes

Vulnérabilités affectant la téléphonie mobile

Les mécanismes de sécurité mis en œuvre dans les systèmes de téléphonie mobile sont découpés en deux volets selon qu'ils concernent les communications entre le mobile et la station de base de proximité ou le cœur du réseau.

GSM et GPRS, définis conjointement par l'ETSI, disposent des mêmes mécanismes visant à assurer la confidentialité de l'identité de l'utilisateur (« *anonymat* »), son authentification et la confidentialité de la communication.

Ces mécanismes s'appuient sur des ***algorithmes non publics***, déployés sur les cartes SIM et le réseau, afin d'authentifier l'utilisateur, de générer les clés de session de chiffrement et de chiffrer. Les algorithmes d'authentification et de génération de clés sont propres à un opérateur et sont implémentés sur le centre d'authentification. L'algorithme de chiffrement est commun à un ensemble d'opérateurs. Il est implémenté sur les stations de base.

Plusieurs faiblesses ont été identifiés sur les réseaux GSM et GPRS [5].

N°	Vulnérabilités
Vul.10.	Faiblesse de l'algorithmes de chiffrement A5 *Les clefs de session de 64 bits sont trop faibles. Certaines implémentations de l'algorithme A5 positionnent les 10 derniers bits à zéro. L'algorithme A5 est officiellement craqué [6] et des sources circulent sur Internet.*
Vul.11.	Absence d'authentification de la station de base *Il est possible de simuler (coût approximatif de 10K€) une fausse station de base, afin d'intercepter les demandes d'authentification et négocier avec le mobile l'absence de chiffrement sur les données.*
Vul.12.	Absence de contrôle d'intégrité si le chiffrement est désactivé *Quelques opérateurs n'effectuent pas de chiffrement sur leur réseau et le recours à de fausses stations de base permet de le désactiver. Les informations ne bénéficient alors d'aucun contrôle d'intégrité.*
Vul.13.	Absence de chiffrement dans le cœur du réseau de l'opérateur *Seules les informations circulant entre le mobile et les stations de base sont chiffrées. Les informations transmises dans le cœur du réseau sont accessibles en clair par les exploitants du réseau.*

Tableau 14 : Vulnérabilités affectant les réseaux GSM et GPRS

Le groupement 3GPP (« *3rd Generation Partnership Project* ») définit les mécanismes de sécurité du réseau UMTS. Ils sont basés sur ceux des réseaux GSM et GPRS pour facilité l'évolutivité vers l'UMTS.

Les principes de sécurité permettant d'assurer les objectifs des réseaux GSM et GPRS ont été conservés. En outre, pour pallier les principales failles des réseaux GSM et GMTS, de nouveaux objectifs en terme de sécurité ont été définis. Il s'agit notamment du renforcement des algorithmes (en s'appuyant sur des algorithmes publics), de l'authentification du réseau et de l'intégrité des données.

Le renforcement de la sécurité de l'UMTS concerne principalement la communication entre le mobile et la station de base et non celle dans le cœur du réseau de l'opérateur.

Les mécanismes de sécurité de l'UMTS n'étant pas complètement définis, il est donc difficile de se prononcer sur les failles ou faiblesses qu'ils présenteront. En revanche, les opérateurs peuvent décider de ne pas suivre entièrement les standards définis par 3GPP. Des failles de sécurité pourraient en résulter.

Vulnérabilités affectant les communications sans fil

Les deux technologies de communication sans fil Bluetooth et 802.11b sont célèbres pour leurs failles de sécurité. Par essence, l'usage des ondes radioélectriques, dont la propagation omnidirectionnelle peut franchir murs et obstacles, facilite :

- Les écoutes passives, qui deviennent pratiquement indétectables.
- Les dénis de service, par perturbation de la bande de fréquence de 2,4GHz que les deux technologies se partagent.

Par ailleurs, les mécanismes de sécurisation retenus ont rapidement montré leurs limitations [10] dans leur utilisation, ainsi que leurs failles [11] dans leur implémentation.

N°	Vulnérabilités
Vul.14.	Partage du code PIN de 4 bits entre plusieurs équipements Bluetooth
Vul.15.	Possibilité de spoofing d'adresse par rejeu de la clef de session (*Link key*)
Vul.16.	Possibilité de spoofing de l'adresse de l'équipement Bluetooth (*Bluetooth Device Address*)
Vul.17.	Faille dans l'implémentation de RC4 dans le protocole WEP de 802.11 (*Wired Equivalent Privacy Protocol*)

Tableau 15 : Vulnérabilités affectant Bluetooth et 802.11b

Vulnérabilités affectant le réseau du ou des opérateurs

L'appréciation des vulnérabilités tient à la confiance que l'on attribue à l'opérateur dans la maîtrise technique de son infrastructure (sécurité des équipements, gestion des configurations, supervision, organisation, etc.) ainsi que dans la fiabilité de son personnel (éthique, moralité, …). Cette problématique est particulièrement renforcée dans un contexte international, dès lors qu'il s'agit de pays « sensibles ».

N°	Vulnérabilités
Vul.18.	Possibilité d'un manque de maîtrise technique de l'opérateur sur son infrastructure
Vul.19.	Possibilité d'une « défaillance humaine » chez l'opérateur *Personnel manipulable, absence d'éthique ou de règles morales…*

Tableau 16 : Vulnérabilités propres aux réseaux opérateurs

Vulnérabilités affectant le réseau Internet

La visibilité qu'offre Internet de l'ensemble de ses nœuds augmente la potentialité des risques identifiés pour les réseaux d'interconnexion (cf. Tableau 10). Les tentatives d'intrusion, de dénis de service, d'altération sont fréquentes sur Internet. En revanche, la probabilité d'une écoute passive est faible (nécessité de disposer d'une complicité chez le ou les ISP de l'entreprise).

N°	Vulnérabilités
Vul.20.	Possibilité d'un manque de maîtrise technique du ou des ISP sur leur infrastructure
Vul.21.	Possibilité d'une « défaillance humaine » chez l'ISP

Tableau 17 : Vulnérabilités propres à Internet

Potentialité d'apparition des menaces selon les modes de raccordement

Les modes de raccordement définis au paragraphe 3.3.1. encourent les menaces du Tableau 10 selon une potentialité différente, fonction des vulnérabilités qui les caractérisent. Le tableau qui suit propose une classification des modes de raccordement selon cette « potentialité » d'apparition.

Mode de raccordement	Potentialité
Liaison permanente entre deux réseaux non publics	Faible
Liaison commutée analogique (RTC) ou numérique (RNIS)	Faible
Téléphonie mobile (GSM, GPRS)	Moyenne
Liaison permanente (ADSL ou modem câble) sur le réseau Internet *Probabilité importante d'occurrence de risque d'attaques (prise de contrôle, dénis de service) ou d'écoute en raison de la permanence de la connexion*	Haute
Communication sans fil (Bluetooth, 802.11b) La portée limitée de Bluetooth (théoriquement 10m., en pratique 3m.) l'expose moins qu'un autre mode de communication sans fil.	Haute

Tableau 18 : Potentialité d'apparition de menaces par nature de raccordement

3.3.3. Éléments à sécuriser, parades

Le réseau d'interconnexion présente des faiblesses à différents niveaux :

- Point de raccordement physique
- Média de transmission physique (paires de cuivre, coaxial, ondes…)

- Réseau du ou des opérateurs (composants, personnel, organisation…)

Selon le mode de raccordement ou le réseau employé, des parades sélectives peuvent être employées. Cependant, parce que le réseau d'interconnexion n'est pas maîtrisé par l'entreprise, les parades doivent, la plupart du temps, être appliquées aux équipements d'extrémité ; c'est à dire, soit à l'équipement terminal, soit à la passerelle d'accès au S.I., soit conjointement aux deux.

N°	Parades
Par.1.	Protection physique des points de raccordement *Par exemple locaux techniques / non applicable pour les accès publics ou les communications sans fil.*
Par.2.	Contrôle d'intégrité des échanges
Par.3.	Authentification forte des parties *Utilisateurs, ressources, équipements d'extrémité*
Par.4.	Chiffrement des communications *Au niveau réseau (VPN IPSec…), au niveau applicatif (SSL/TLS…)*
Par.5.	Cloisonnement des informations et des applications *Réduction du périmètre applicatif et de données accessibles par les utilisateurs en recourant à la restriction des droits d'accès.*
Par.6.	Clauses contractuelles avec l'opérateur *Dans le cas d'offres nomades opérateur…*

Tableau 19 : Parades relatives au réseau d'interconnexion

3.4. PASSERELLE D'ACCES AU SI

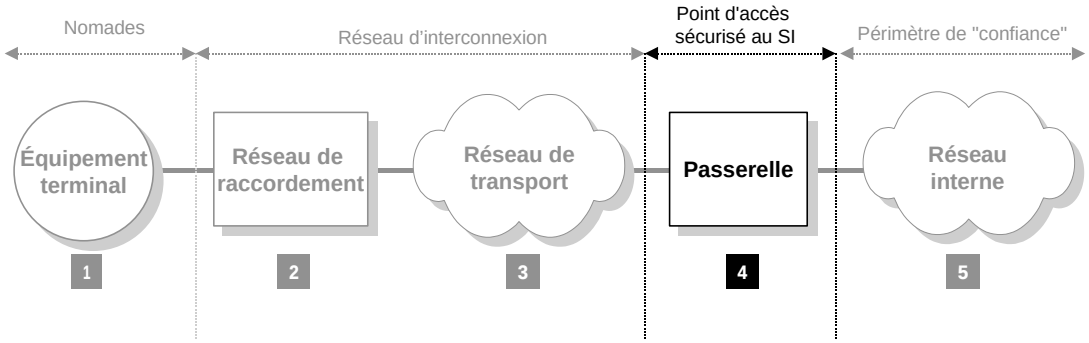

Figure 4 : Passerelle d'accès au S.I.

3.4.1. Définition

La passerelle d'accès sécurisé au système d'information est l'ensemble des moyens matériels et logiciels qui assurent l'accessibilité de tout ou partie des ressources du S.I. de l'entreprise et en garantissent la non compromission (en termes de disponibilité, d'intégrité, de preuve et confidentialité). Cette accessibilité obéit à une politique de sécurité définie par l'entreprise.

L'architecture de la passerelle d'accès est dictée par :

- Les besoins et moyens de raccordement, définis par l'entreprise, en adéquation avec les réseaux de raccordement et de transport qu'elle emploie.

  En la matière, de nombreuses variantes sont envisageables compte tenu de la variété des offres des opérateurs télécoms et de la combinatoire des moyens de raccordement.

- Des considérations sécuritaires, adaptées à la sensibilité des informations du S.I. (ou des ressources mises à disposition) et aux moyens de raccordement sélectionnés.

Cette richesse de composition rend difficile une classification des passerelles d'accès. Néanmoins, il est possible de dégager trois grands profils[4] de passerelles :

- Passerelle type « RAS »
- Passerelle type « Réseau Privé Virtuel »
- Passerelle type « Internet »

Passerelle « RAS »

La passerelle de type « RAS » est raccordée aux réseaux téléphoniques publics (analogiques ou numériques). Elle englobe les services d'accès distants « RAS », par lesquels l'entreprise assure directement l'établissement de la connexion des utilisateurs (niveau 2 du modèle OSI).

Les serveurs d'accès distants sont généralement possédés en propre par l'entreprise qui met à disposition de ses nomades un ou plusieurs numéros d'appels locaux ou nationaux. Ce type de passerelle convient moins aux contextes internationaux (compte tenu des coûts de télécommunications) ou à forte population (densité des appels).

Passerelle « Réseau Privé Virtuel »

La passerelle de type « Réseau Privé Virtuel » est raccordée à un réseau d'opérateur télécoms, dans le cadre d'une offre RPV (exemple, Global Intranet d'Equant).

Ce type d'offre permet de « construire » une extension du réseau de l'entreprise en s'appuyant sur celui de l'opérateur (Frame Relay, MPLS…) tout en proposant des modalités de raccordement standard aux utilisateurs nomades et itinérants (RTC, RNIS, GSM, ADSL).

Le périmètre de couverture est généralement de dimension nationale, continentale voire internationale grâce aux points de présence (POP) de l'opérateur dans les différents pays.

Ce type d'offre intègre également des solutions de sécurité qui complètent ou interagissent avec celles de l'entreprise, notamment pour l'authentification des utilisateurs nomades (RADIUS).

[4] Cette classification ne se veut évidemment pas exhaustive.

Passerelle « Internet »

La passerelle de type « Internet » est raccordée à Internet par le biais d'un fournisseur d'accès ISP. L'interconnexion de type « full IP » assure à l'entreprise une visibilité et une accessibilité internationale, adaptée au grand nomadisme, tout en garantissant des coûts de communication modérés souvent forfaitisés.

Là encore, les mécanismes de sécurité sont très variés selon les risques identifiés et leur potentialité : authentification, habilitation, contrôle des flux, protection anti-virale et contrôle des contenus, sécurisation des échanges, détection d'intrusion…

3.4.2. Problématiques de sécurité

Analyse de la sensibilité d'une passerelle d'accès

L'évaluation de la sensibilité d'une passerelle d'accès relève d'une démarche d'audit de sécurité. En cela, il est difficile de qualifier, dans le cadre du présent document, la sensibilité d'une passerelle dans l'absolu. Aussi nous proposons, plutôt, d'examiner les principaux facteurs qui caractérisent, d'un point de vue sécuritaire, la sensibilité d'une passerelle :

- Éléments de communication et de sécurisation.

  De manière inhérente à leur conception, ces éléments comportent potentiellement des vulnérabilités d'origines diverses ; bogues de développement, configuration par défaut, erreurs dans l'implémentation d'un protocole (dont la spécification est insuffisante), qualifications techniques insuffisantes, etc.

  La sélection des éléments de communication et de sécurisation (pilotée notamment par la fiabilité, la pérennité et les coûts des produits), constitue une étape importante dans la construction de la passerelle d'accès.

- Architecture de la passerelle

  L'architecture de la passerelle peut constituer, en soit, un élément de fragilisation de la passerelle d'accès ; une architecture mal conçue ou trop complexe (définition des périmètres de sécurité, agencement des composants, identification des flux, …) peut introduire des vulnérabilités pouvant exposer des éléments importants de la passerelle d'accès.

- Règles d'administration et d'exploitation

  Les règles d'administration et d'exploitation des éléments de communication et de sécurité visent à garantir non seulement le bon fonctionnement de la passerelle d'accès mais également à maintenir son niveau de sécurité. L'incomplétude des règles et leur non-application risquent d'introduire des vulnérabilités (processus de validation incomplets, erreurs de configuration, absence de mises à jour, …), surtout dans le contexte d'une architecture complexe.

- « Actualité » de la passerelle

  L'absence de mise à jour des composants logiciels est un facteur dégradant de la sécurité de la passerelle. Régulièrement des failles ou des bogues sont identifiées sur les composants, que des attaquants ont la capacité d'exploiter.

En outre, l'évolution des technologies amène à l'emploi de nouveaux outils, voire de nouvelles pratiques de la sécurité. L'architecture et les règles de gestion méritent d'être donc régulièrement auditées.

Niveau de sécurité de la passerelle d'accès

Nous appelons « niveau de sécurité » de la passerelle d'accès, le niveau de sécurité que lui procure son architecture et ses éléments de sécurité. Ce « niveau de sécurité » est le fruit de l'analyse des risques que présente, intrinsèquement, la chaîne de communication reliant les utilisateurs itinérants / nomades à la passerelle d'accès.

Pour reprendre la typologie de passerelles évoquées au paragraphe 3.4.1. , les chaînes de communication « VPN », « RAS » et « INTERNET » présentent chacune un niveau différent de risques, combinaison des risques détectés ou pressentis pour chacun des maillons les constituant. Une analyse macroscopique conduit, donc, à accorder des niveaux différents de confiance à ces chaînes ; niveaux qui, a priori, n'atteignent pas celui attendu par l'entreprise (cf. schéma d'illustration suivant).

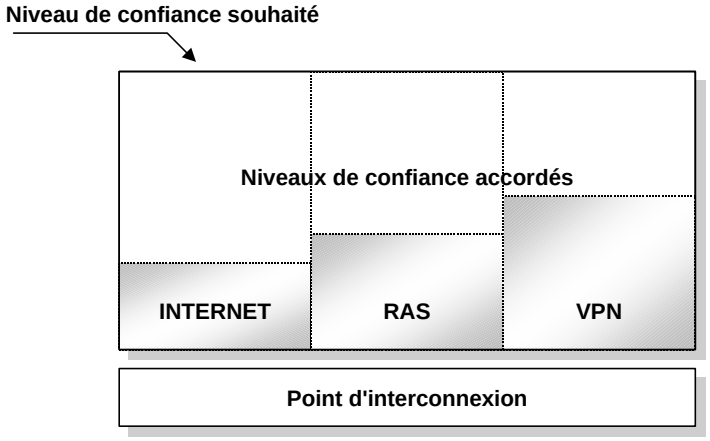

Figure 5 : Exemple du niveau de confiance accordé par chaîne de liaison

L'élaboration d'une passerelle d'accès d'un type donné prend donc en considération le niveau de confiance accordé à la chaîne d'interconnexion associée, afin de pallier les risques qu'elle présente et atteindre un niveau de sécurité attendu par l'entreprise. Ainsi, pour atteindre un même niveau de sécurité cible, les trois types de passerelle doivent s'appuyer sur des architectures de sécurité de complexité variable.

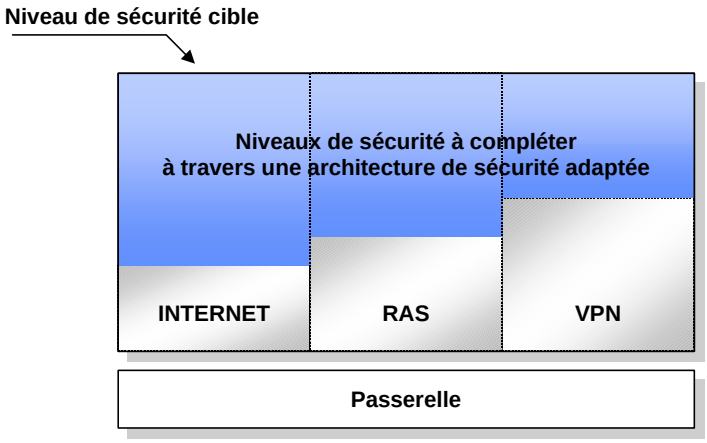

Figure 6 : Exemple du niveau de sécurité atteint par type de passerelle

Menaces pesant sur la passerelle d'accès au S.I.

La passerelle d'accès au S.I. est une architecture de composants matériels et logiciels sur lesquels pèsent un certain nombre de menaces.

N°	Menaces	Impacts			
		D	I	C	Poids
Men.1.	Défaillance technique d'équipements *Panne matérielle / Dysfonctionnement matériel ou logiciel*	✓			2
Men.2.	Détérioration physique d'équipements	✓			1
Men.3.	Altération de composants logiciels	✓	✓	✓	1
Men.4.	Accès illicites *Usurpation de droits…*		✓	✓	3
Men.5.	Infection *Virus, ver, chevaux de Troie*		✓	✓	1
Men.6.	Prise de contrôle d'un équipement réseau ou de sécurité *Chevaux de Troie / exploitation de failles / défauts de configuration*	✓		✓	3
Men.7.	Déni de service	✓	✓	✓	3
Men.8.	Divulgation d'information			✓	3
Men.9.	Rebond *rebond sur certains services (messagerie, shell, transfert de fichiers)*	✓		✓	3

Tableau 20 : Menaces pesant sur la passerelle d'accès au S.I.

La pondération signifie :

1) Potentialité d'occurrence faible : la menace ne constitue pas un réel danger.

2) Potentialité d'occurrence moyenne : si ses conséquences sont redoutées, certaines parades peuvent s'avérer utiles pour s'en prémunir.

3) Potentialité d'occurrence haute : si ses conséquences sont redoutées, il est indispensable de mettre en œuvre les parades pour s'en prémunir.

Vulnérabilités

Les composants de la passerelle présentent des faiblesses de par leur conception, leurs modes de fonctionnement, leur utilisation ou même de leur agencement.

N°	Vulnérabilités
Vul.1.	Présence de failles sur les composants de la passerelle *Bogues des logiciels, erreurs d'implémentation...*
Vul.2.	Mauvaise configuration des équipements
Vul.3.	Défauts dans l'architecture de la passerelle *Filtrage inadéquat, absence de zones de sécurité cloisonnant les services*
Vul.4.	Erreurs, négligences ou défauts d'exploitation *Inadéquation ou absence de procédures de supervision, de maintenance…*

Tableau 21 : Vulnérabilités affectant la passerelle d'accès au S.I.

3.4.3. Éléments à sécuriser, parades

Tous les éléments constitutifs de la passerelle, y compris l'architecture de la passerelle, sont concernés par l'application de mesures de prévention et de protection, dont font partie les parades suivantes :

N°	Parades
Par.1.	Protection physique des équipements et des locaux
Par.2.	Authentification forte des utilisateurs
Par.3.	Chiffrement des communications *Au niveau réseau (VPN IPSec…), au niveau applicatif (SSL/TLS…)*
Par.4.	Filtrages et contrôles de contenu
Par.5.	Contrôle d'intégrité des échanges
Par.6.	Détection d'intrusion
Par.7.	Mécanismes de haute disponibilité
Par.8.	Cloisonnement des informations et des applications *Réduction du périmètre applicatif et de données accessibles par les utilisateurs / constitution de zones de sécurité*
Par.9.	Mise en place d'une cellule de veille sécuritaire
Par.10.	Audits d'architecture et mesures de vulnérabilité

Tableau 22 : Parades relatives à la passerelle d'accès au S.I.

3.5. RESEAU INTERNE

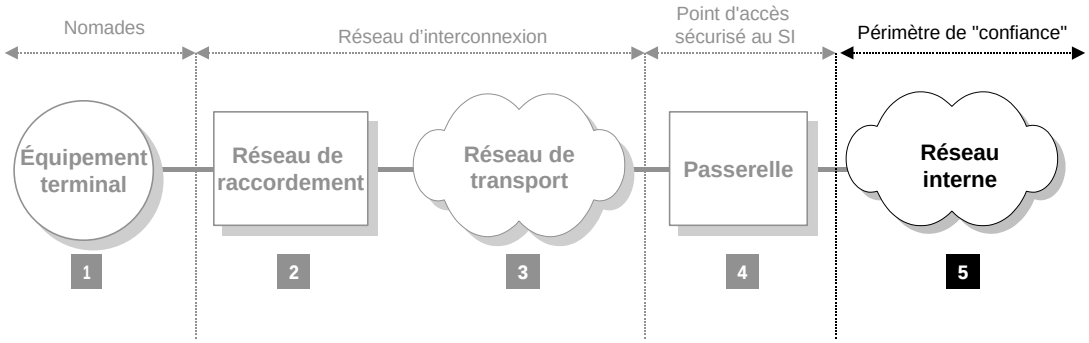

Figure 7 : Réseau interne

3.5.1. Définition

Par définition, le réseau interne de l'entreprise constitue l'ensemble des moyens matériels et logiciels assurant la connectivité au système d'information, c'est à dire aux ressources applicatives et aux données de l'entreprise.

Le réseau de l'entreprise est considéré, dans le cadre de ce document de synthèse, comme le « périmètre de confiance » de l'entreprise, tant en termes de :

- Protection physique (des équipements, des locaux…) et logique.
- Identification physique et logique (des équipements, des personnels…).
- Maîtrise des infrastructures techniques du réseau interne.
- Habilitation des utilisateurs.
- Politique de sauvegarde des données.
- …

L'analyse des menaces et des vulnérabilités qui pèsent sur le réseau interne et des parades à y opposer ne fait pas l'objet du présent document.

4. APPROCHE DE SECURISATION

Ce chapitre propose aux lecteurs une approche conduisant à sécuriser les accès au système d'information de l'entreprise par le personnel en déplacement hors de son lieu de travail.

4.1 DEMARCHE

Une approche globale peut être conduite en quatre étapes successives, autant pour mettre en place un nouveau système de nomadisme, ou pour étendre ou améliorer un système existant. Ces quatre étapes sont décrites ci-dessous :

Étape 1 : Recenser ou analyser les scénarios de raccordement

Cette première étape conduit à établir un catalogue des solutions pouvant être mises en œuvre dans l'entreprise et un recensement des mécanismes déjà mis en place. (cf. 3.1).

Étape 2 : Identifier les populations nomades et l'utilisation effective

L'analyse doit principalement porter sur les éléments suivants :

- Quelles sont les catégories et les métiers utilisant le nomadisme, ou candidats à cette fonction (direction, personnel commercial, …) ?
- Quelles sont les fréquences et exigences de qualité de service ? Quelle est la sensibilité des informations et des applications concernées ? Cette analyse peut se référer à une classification existante, mais elle nécessite toujours d'une analyse de risque complémentaire.
- Quelles sont les limites d'utilisation effectives ou supportables (droits en lecture, en écriture, en import, …) ?

Étape 3 : Identifier les vulnérabilités et risques effectivement présents

Les menaces seront analysées et les vulnérabilités mises en évidence, notamment :

- Les vulnérabilités « système » (version d'OS, …).
- Les vulnérabilités techniques et fonctionnelles des applications (applications standard et applications propriétaires, …).
- Les vulnérabilités liées aux modes d'utilisation (modes d'authentification, procédures d'accès à distance, …).
- Les vulnérabilités liées aux conditions d'administration et d'exploitation (traçabilité des accès, détection et gestion des incidents, procédures d'administration et de maintenance…).

Étape 4 : Déterminer les parades pertinentes et le plan d'action de sécurisation

Les modalités de mise en œuvre seront adaptées à la politique de sécurité de l'entreprise, au plan d'action / projets de sécurisation éventuels, aux contraintes fonctionnelles identifiées lors de l'étape 2, aux exigences budgétaires, …

Le plan d'action peut comprendre trois types de mesures :

- Parades techniques (ensemble des outils à positionner sur tout ou partie des maillons de la chaîne).
- Parades organisationnelles (cellule de veille sécuritaire, organisation de la cellule sécurité, procédures fonctionnelles d'accès distants, sensibilisation des utilisateurs et formation des administrateurs…).
- Parades contractuelles (vis à vis de l'opérateur, du tiers mainteneur, des constructeurs et fournisseurs).

4.2 POLITIQUE DE SECURITE DES ACCES

L'efficacité des moyens techniques de sécurité mis en œuvre est conditionnée par une bonne sensibilisation des utilisateurs et une formation des administrateurs des systèmes d'information.

Il est ainsi indispensable d'appliquer une politique formelle de protection des accès par les populations nomades. Ce document formel doit être élaboré en cohérence avec la politique de sécurité de l'entreprise. Il doit être mis en application par la Direction, et son application doit être régulièrement contrôlée.

Cette politique pourra notamment comporter les éléments suivants :

- Champ d'application de la politique.
- Objectifs, enjeux et risques liés aux accès nomades.
- Obligations et exigences de sécurité, notamment en matière de protection de la confidentialité et de l'intégrité des informations, de disponibilité des systèmes, d'intégrité des informations et des traitements.
- Responsabilités des acteurs dans le cadre des accès nomades (exploitants, utilisateurs, propriétaires des informations / applications, équipe sécurité, auditeurs, …).
- Présentation des règles et procédures de sécurité applicables, liées à l'utilisation des moyens d'accès et aux activités d'administration et d'audit.
- Règles et procédures de suivi et de gestion des incidents de sécurité.
- Principes de traçabilité et d'audit.
- Règles d'évolution de la politique de sécurité.

Cette politique de sécurité pourra être déclinée en deux documents distincts :

- La Charte de sécurité des accès nomades, destinée aux acteurs du système d'information (RSSI, maîtrise d'ouvrage, maîtrise d'œuvre, administrateurs et exploitants, …).
- Les règles de sécurité des accès nomades (document synthétique d'environ 1 page) destiné à l'ensemble des utilisateurs concernés.

REFERENCES

[1] Laura Thomas, “Vulnerabilities in the PalmOS version 3.x”, SANS Institute, juillet 2001.

[2] Dave Croxton, “PDAs in the Corporate Environment”, SANS Institute, septembre 2001.

[3] WAP Forum, “Wireless Application Protocol – Wireless Transport Layer Security (WTLS) Specification, version 12-feb-1999”, www.wapforum.org , 1999.

[4] Markku-Juhani Saarinen, “Attacks against the WAP WTLS protocol”, Univerisity if Jyväskylä, Finland, 2000.

[5] Michael Schmidt, “Consistent M-Commerce Security on Top of GSM-based Data Protocols – A security Analysis”, University of Siegen, Germany, 2001. http://www.mobilesummit2001.org/mcs2001/papers/MOBCS4VWBFE.pdf

[6] Alex Biryykov, Adi Shamir, “Real Time Cryptanalysis of GSM A5/1 on a PC”, http://cryptome.org/a51-bsw.htm , avril 2000.

[7] Juha Vaino, “Bluetooth Security”, Helsinki University of Technology, mai 2000.

[8] M.Jakibsson, S.Wetzel, “Security weakness in Bluetooth”, www.bell-labs.com/user/markusj/bt.html , 2001.

[9] Cathal Mc Daid, “Bluetooth Security – Evaluation & Conclusion”, www.palowireless.com , mars 2001.

[10] Sultan Weatherspoon, “Overview of IEEE 802.11b Security”, Intel Technology Journal, Q2 2000.

[11] ISS, “Wireless LAN Security, 802.11b and Corporate Networks”, Internet Security Systems, 2001.