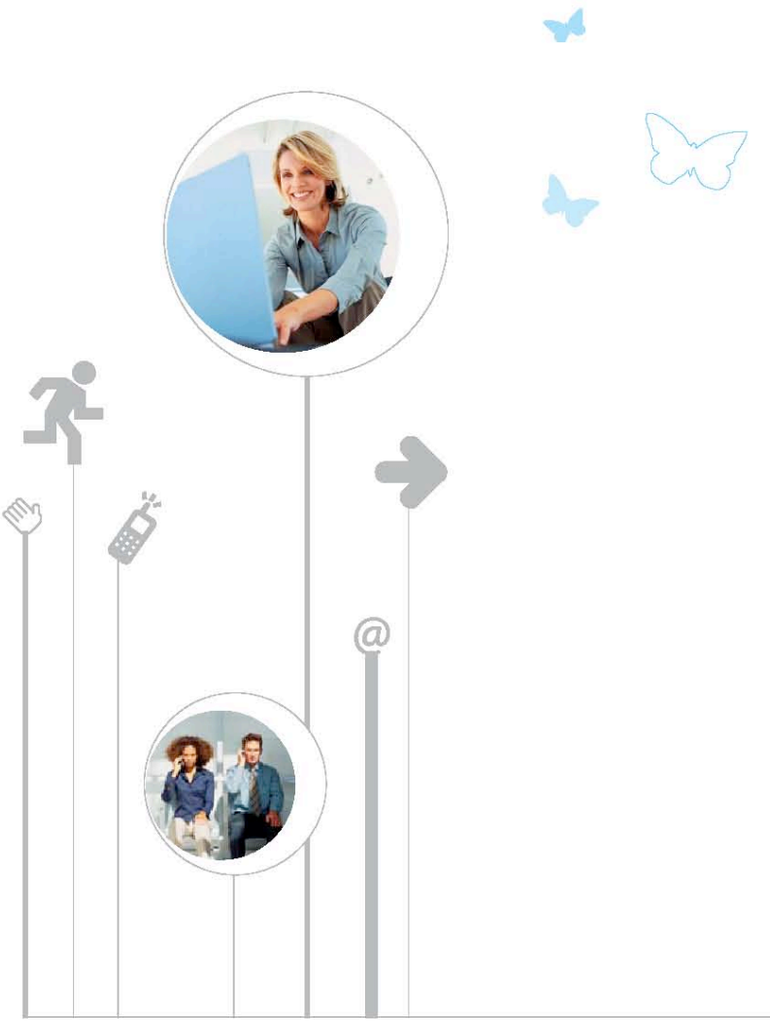
Livre blanc **de la Mobilité et de la Sécurité** V1.0 14 AVRIL 2006



Conçu et réalisé par la Chambre Monégasque des Nouvelles Technologies de l'Information et de la Communication et le concours de Messieurs Svend Albertsen, Olivier Merlin et Éric Perodeau.

Sponsorisé par le groupe de courtage d'assurances et de réassurances Ascoma, l'éditeur de solutions de sécurité Check Point, la banque CFM (Crédit Foncier de Monaco), le groupe Microtek, le registrar et société de services Namebay, l'intégrateur de technologies Novenci, l'intégrateur de solutions de sécurité et mobilité Tekworld.

NTIC Chambre Monégasque des Nouvelles Technologies de l'Information et de la Communication

GROUPE ASCOMA Courtage d'Assurances et de Réassurances

Check Point SOFTWARE TECHNOLOGIES LTD. We Secure the Internet.

CFM MONACO

GROUPE Microtek

NOVENCI MONACO

colibri

conception - réalisation : www.colibri.mc

LES AUTEURS

Svend Albertsen est Consultant en Informatique et Réseaux, spécialisé en sécurité informatique et Internet ainsi que dans les systèmes d'exploitation réseau Windows/Unix/Linux. Il est également membre de la Chambre des Experts de la Principauté de Monaco.

Olivier Merlin est Directeur Technique de la société Tekworld (groupe Microtek), ISP et WISP, spécialisé dans l'architecture IP, Systèmes, Sécurité et Mobilité.

Eric Perodeau est Directeur Général de la société Media Computers SSDI, société de services et de distribution spécialisée dans les domaines de la mobilité, la sécurité et le rich-media en particulier.

LES PARTENAIRES

CFM MONACO

GROUPE Microtek

NOVENCI MONACO

colibri

TEKWORLD

GROUPE Microtek

GROUPE ASCOMA
Courtage d'Assurances et de Réassurances

namebay
créateur de noms de domaine

Check Point
SOFTWARE TECHNOLOGIES LTD.
We Secure the Internet.

Un monde changeant, un monde évolutif à grande vitesse, des technologies toujours plus complexes et pourtant de plus en plus abordables à tout un chacun, c'est notre monde actuel.
L'informatique n'y échappe pas, elle est même un des leaders de ce changement. Depuis ses débuts avec les calculateurs mastodontes, nous avons vu arriver de la micro-informatique, d'abord isolée, puis en réseau local et maintenant Internet.
De son côté, la téléphonie a aussi connu une évolution phénoménale, du 22 à Asnières au téléphone moderne, en y ajoutant la notion de mobilité, le téléphone portable radio puis GSM.
Parallèlement, l'industrie informatique avait elle aussi tenté la mobilité avec des PC de format machine à coudre, plus transportables que portables.
La technologie moderne nous a amené au PC portable actuel, et les progrès de la miniaturisation ont donné naissance aux assistants personnels (PDA).
Nous assistons maintenant à la convergence des deux mondes, l'informatique et la téléphonie.
D'abord grâce aux progrès de la numérisation de la voix, qui devient alors de la donnée numérique à transporter, mais surtout au mélange des deux technologies dans des matériels de plus en plus petit tels que les téléphones assistants intelligents Smartphone.
Ainsi, grâce à un vaste choix de matériels et des techniques, nous sommes maintenant capables d'accéder à la liste complète de ses contacts, ses rendez-vous, sa messagerie et même l'ensemble de son système d'information, à distance !
Ce n'est qu'un problème d'expression des besoins, de mise en place des solutions appropriées, avec le conseil de professionnels du métier.
Ce livre blanc a pour mission de vous présenter les diverses solutions technologiques de mobilité, sans entrer dans un domaine trop technique, mais aussi de vous mettre en garde contre les risques auxquels ces nouvelles possibilités vous exposent.
Un certain nombre de termes techniques et d'abréviations sont expliqués dans le lexique.

1. LES BESOINS

1.1 – DONNÉES PERSONNELLES

Tout commence souvent avec une problématique simple, partagée aussi bien par le grand public que par le monde du travail : le carnet d'adresses et l'agenda.
Si on laisse de côté les irréductibles du papier, on garde souvent dans son PC la liste de ses contacts et son agenda ; mais on peut avoir un PC au bureau et un à la maison, voire même un PC portable, voire en plus un PDA et/ou un téléphone GSM.
Là, la solution viendra d'un logiciel de synchronisation, généralement fourni avec les appareils concernés qui demandera d'être certainement mis à jour dans le cadre d'une synchronisation avec une messagerie d'entreprise comme Microsoft Exchange ou Lotus Domino, ces produits ayant déjà en eux-mêmes les fonctionnalités nécessaires à l'échange des données de contact et d'agenda.

1.2 – LES DONNÉES DE GROUPE

La situation se complique, car il n'est pas aussi facile de synchroniser tous les contacts de l'entreprise et les agendas de groupe des collaborateurs : on préférera alors plutôt se connecter à distance au système d'information pour consulter ces données.
Deux approches sont possibles :
• soit utiliser un client lourd (le logiciel fourni par les éditeurs de la solution) comme par exemple un client Lotus Notes, et le connecter à distance par le moyen adéquat,
• soit utiliser un client léger (typiquement un navigateur Internet) qui donnera plus de souplesse car disponible sur à peu près tous les matériels, cette deuxième solution à de plus l'avantage de ne pas avoir à installer de logiciels, et donc de pouvoir être facilement utilisé sur un PC de maison, un PDA, une machine libre-service dans un aéroport ou un cybercafé.

1.3 – LA MESSAGERIE

Autant les données personnelles évoquées précédemment sont peu mobiles et ne demandent qu'une synchronisation régulière, autant la messagerie pose de nouveaux problèmes car elle vit tout le temps :
• Comment consulter ses messages de n'importe où ?
• Est-il indispensable de pouvoir répondre de n'importe où ?
• Comment être averti si un message nouveau est arrivé ?

1.3.1 – COMMENT CONSULTER SES MESSAGES DE N'IMPORTE OÙ ?

Un programme de messagerie classique tel que Microsoft Outlook Express livré avec toutes les versions de Windows est l'outil classique que tout un chacun utilise pour consulter la messagerie offerte par son fournisseur d'accès Internet avec son abonnement : on parle habituellement de messagerie POP3, c'est à dire que les messages arrivés pour vous chez votre fournisseur attendent sagement que vous veniez les chercher en les transférant dans votre PC ; vous êtes alors détenteur de vos messages, dans une seule machine, il devient évident que ces messages ne pourront désormais être consultés que sur cette machine ! Un début de mobilité peut consister à synchroniser une partie de cette messagerie avec un PDA/Smartphone, mais ce système montre vite ses limites.
Dans le cadre d'une messagerie d'entreprise, qui est centralisée dans les serveurs de messagerie, on ne retire plus ses messages, on les consulte avec les outils appropriés :
• soit le client de messagerie lourd fournie par l'éditeur (Microsoft Outlook, Lotus Notes) qui possède en lui-même des fonctions dites de synchronisation /réplication, vous permettant alors de partir avec tout ou partie de votre messagerie (selon vos critères).
• soit un client de messagerie léger, qui supporte un protocole appelé IMAP (et non plus POP3), et qui permet alors de consulter et synchroniser tout ou partie de sa messagerie (généralement les derniers messages) sur différents types de matériels (PC multiples, PDA, GSM, Smartphone) sans retirer les messages du serveur d'entreprise.

• soit un client léger de type webmail, tout simplement accéder à sa messagerie par un simple navigateur Internet, et ce de n'importe où, avec n'importe quel matériel possédant un navigateur, à ceci près que la lisibilité soit assurée (pas d'écran trop petit). Les grands de la messagerie gratuite offrent d'origine de tels accès (Yahoo!mail, Hotmail, etc.), mais les grands éditeurs de solution de messagerie d'entreprise (Microsoft, Lotus) offrent aussi l'accès webmail.

Il est important de prendre en compte le cas des fichiers rattachés (pièces jointes) : ils imposent deux contraintes, celle de la taille et celle de la visualisation. Des matériels à capacité limitée n'ont pas forcément la possibilité de récupérer les pièces jointes suivant leur taille de leur mémoire ou leur vitesse de communication, d'autres n'ont tout simplement pas les logiciels nécessaires pour les visualiser (GSM). Le traitement des pièces jointes restera généralement réservé à des matériels de grande taille (PC portable, voire PDA grands formats).

De ses différentes méthodes, on pourrait dresser à titre d'exemple un petit scénario de l'homme moderne connecté à sa messagerie :
équipé par la direction du système d'informations d'un ordinateur portable, il l'utilise en tant que poste fixe à son bureau : il consulte sa messagerie en direct avec son serveur de messagerie et est averti au fil de l'eau des messages arrivés ; appelé en réunion, il débranche son câble réseau et met en marche son réseau sans fil Wi-Fi, pour continuer à gérer sa messagerie centralisée pendant la réunion. Le soir, avant de partir, il lance une synchronisation de sa messagerie sur son portable, et peut dès lors consulter l'historique de ses messages envoyés et reçus jusqu'au moment de la synchronisation. Pendant son trajet, il démarre le client léger de messagerie de son téléphone portable afin de consulter sommairement les derniers messages reçus, éventuellement d'y répondre en quelques mots. Arrivé à la maison, son portable reconnecté à son bureau par l'intermédiaire de sa connexion ADSL personnelle, il peut à nouveau soit travailler au fil de l'eau, soit synchroniser à la fréquence voulue sa messagerie pour y travailler ensuite en mode déconnecté.

Évidemment, ce scénario n'est qu'un exemple, on peut imaginer se passer de PC portable, utiliser un PDA communicant/Smartphone, de nombreuses possibilités sont offertes.

1.3.2 – RÉPONDRE DE N'IMPORTE OÙ ?

Tous les clients de messagerie permettent de répondre, la limitation vient plutôt de la facilite de frappe clavier : un téléphone portable n'offre que peu de touches (avec plusieurs lettres par touche) qui, même avec des techniques modernes, s'avèrent fastidieuses pour écrire longuement ; on se limitera alors à la frappe de quelques mots. Un PDA/Smartphone peut être doté d'un vrai petit clavier Azerty, donnant alors plus de souplesse, mais restant quand même limité en confort pour une réponse détaillée. Seul le PC portable ou TabletPC à reconnaissance d'écriture peut permettre de répondre de manière souple, et pouvoir envoyer des pièces jointes conséquentes.

1.3.3 – ÊTRE AVERTI DES MESSAGES ARRIVÉS ?

Dans ce cas de figure, le but n'est plus d'interroger régulièrement sa messagerie, mais d'être averti de l'arrivée d'un nouveau message, comme le font les opérateurs de téléphonie GSM à l'aide des SMS, mais aussi d'accéder directement au contenu des messages. On parle alors de Pushmail. Diverses solutions existent, mais il faut prendre conscience qu'elles demandent une connexion permanente : un des acteurs majeurs de ces solutions, la société américaine RIM, dispose d'un téléphone intelligent nommé Blackberry : l'appareil profite alors de sa connexion permanente téléphonique GSM/GPRS pour dialoguer avec son serveur qui se trouve alors généralement à côté du serveur de messagerie d'entreprise. L'utilisateur a alors un téléphone doublé d'un outil de messagerie sur lequel il visualise en temps réel les messages reçus. L'outil est pour l'instant dédié à la messagerie et n'offre pas d'autre possibilité comme un PDA ou un Smartphone, mais a été choisi comme outil de mobilité par de nombreuses entreprises comme étant suffisant pour les besoins de messagerie mobile. Microsoft vient de finaliser un équivalent pushmail sur les plates-formes Windows Mobile et RIM devrait aussi donner le jour à une version pour Windows Mobile.

1.4 – ACCÈS AUX APPLICATIONS INTRANET DE L'ENTREPRISE

Ce cas de figure est un des plus simple à traiter si l'entreprise utilise des applications qui ont été développées autour des technologies de navigateur Internet, alors elles sont accessibles par essence même de l'extérieur. Un simple navigateur permettra de les utiliser : il faudra quand même prendre en compte les contraintes d'écran des petits terminaux types PDA, voire faire développer alors des écrans spécifiques adaptés aux petites tailles qui simplifieront ainsi la visualisation. Si l'on dispose d'applications sur des ordinateurs centraux ou départementaux, les programmes d'émulations de terminaux sont désormais aussi disponibles en mode web.
L'entreprise doit tout de même se poser quelques questions en ce qui concerne accès distant à des applications internes et les risques associés : quid de la confidentialité des données ? Comment être sûr de l'identité de l'utilisateur qui se connecte ? Ces types de questions trouveront leur réponse dans la deuxième partie du livre blanc, risques et solutions.

1.5 – ACCÈS AUX APPLICATIONS INTRANET DE L'ENTREPRISE

Classiquement, un utilisateur est connecté dans son entreprise à un serveur de fichiers via un réseau local. Il y stocke ses documents dans un répertoire personnel, mais accède aussi à des documents communs à son groupe de travail, bénéficiant ainsi de la sauvegarde centralisée de ces fichiers. Pour partir avec certains de ces fichiers, il doit alors les dupliquer sur son PC portable pour y travailler ailleurs, et surtout ne pas oublier de recopier les fichiers ainsi modifiés à son retour. Il existe des outils facilitant ce genre de travail, par exemple le Porte-documents de Microsoft Windows, l'inconvénient principal est qu'il faut prévoir à l'avance ce dont on pourrait avoir besoin. L'alternative à cette approche est simplement de pouvoir se connecter à distance à ses ressources réseau contenant les fichiers désirés, comme si on était dans son entreprise alors qu'on est en fait à distance vraisemblablement via Internet. En étendant ainsi son réseau d'entreprise jusqu'à son poste mobile distant via un réseau public comme Internet, on crée alors ce que l'on appelle un réseau privé virtuel (RPV ou encore VPN, Virtual Private Network).
Le poste mobile se trouve alors comme s'il était dans le réseau local de l'entreprise, et l'utilisateur peut alors accéder à ses ressources réseau, fichiers et même imprimantes !
Évidemment, cela constitue une ouverture fantastique, on peut alors travailler ailleurs (chez soi, à l'hôtel, en déplacement) comme si on était au bureau, avec une limitation et un risque majeur :
• la limitation est la vitesse, le goulet d'étranglement se situant généralement au débit de sortie des informations de l'entreprise : si l'on prend exemple à Monaco un abonnement ADSL classique à 4.2 Mbps, le débit maximum en sortie (upload) est de 320 Kbps, ce qui donnera concrètement un temps d'accès de l'ordre d'une trentaine de secondes à un simple document bureautique, et si celui-ci contenait aussi des données comme par exemple des images, cela pourrait aisément dépasser plusieurs minutes : dans ce cas, on préféra alors copier le fichier localement, travailler dessus et le renvoyer une fois modifié.
• le risque est celui de l'ouverture totale au réseau et à ses ressources à un utilisateur distant : si celui-ci n'était pas celui qu'il prétend être ou si la connexion venait à être piratée, on imagine aisément les dégâts possibles.
Pour établir un tel réseau VPN, on peut avoir installé un client lourd VPN à l'aide du spécialiste, mais dans ce cas on ne peut accéder au réseau de l'entreprise qu'à partir d'une machine spécialement préparée à cet effet. Une variante du client VPN lourd qui commence à se répandre est le client réseau privé virtuel léger, le VPN SSL. On profite alors un simple navigateur Internet d'un poste non préparé, et la connexion aux ressources réseau de l'entreprise se fait alors via le navigateur : une fois la connexion établie, on accède aux ressources désirées.
Dans ce mode-là, on traitera une attention toute particulière à la sécurité du poste qui justement n'a certainement pas été fourni par des services informatiques (machines personnelles, machines d'un ami, libre-service, etc.).

1.6 – UTILISATION DE PROGRAMMES SPÉCIFIQUES MÉTIER (COMPTABILITÉ, STOCK, GESTION COMMERCIALE, ETC.)

Dans ce cas, une petite étude sera réalisée avec des éléments à prendre en compte comme :

- l'applicatif peut-il être installé sur le poste nomade, doit-il être accédé à distance ?
- les données qu'il véhicule sont-elles volumineuses et compatibles avec le débit envisagé ?

Généralement, une petite maquette prouvera la faisabilité ou l'impossibilité.

1.7 – ACCÈS À UNE SESSION OU UN ORDINATEUR DISTANT

Avec cette approche, la philosophie de la connexion change radicalement : tout le travail s'effectue sur un serveur (voire un poste) au sein de l'entreprise, et l'utilisateur nomade ne transporte plus avec lui que l'équivalent d'un écran/clavier/souris de longueur inhabituelle, des milliers de kilomètres si nécessaire. En fait, c'est comme s'il laissait son ordinateur professionnel au bureau, pilotait de loin le clavier et la souris, et que seule l'image écran de ce qu'il fait à distance lui revenait.

Là, toutes les données du problème changent :

- la vitesse de ligne devient peu importante, car les seuls éléments à véhiculer sont les touches clavier frappées et les mouvements de souris à envoyer, et les mises à jour des parties d'écran modifiées à recevoir,
- la sécurité reste primordiale ainsi que l'identification de l'utilisateur qui se connecte,
- mais le matériel nomade doit impérativement disposer de surface d'affichage suffisante pour travailler, ce qui exclut tous téléphones intelligents de type Smartphone, qui admet avec beaucoup de limitation des PDA, et qui a surtout besoin d'une vraie machine classique avec une résolution d'écran raisonnable.

De plus, toutes les applications nécessaires sont alors installées localement par le service informatique, et il n'y a plus aucune limitation d'utilisation. Les solutions Citrix et Microsoft Terminal Serveur sont de grands exemples de ce type de solutions en mode serveur ; pour le poste à poste, des logiciels comme VNC, Dameware, PCAnywhere de Symantec sont des solutions possibles avec une installation minimum, qui donne alors accès au poste de l'utilisateur resté dans l'entreprise.

1.8 – LA TOIP (TÉLÉPHONIE VIA IP, VOIR NOTRE PREMIER LIVRE BLANC)

Si l'entreprise s'est équipée d'un système de téléphonie IP, l'utilisateur peut alors utiliser soit un téléphone logiciel (Smartphone), soit un téléphone IP pour se connecter au système téléphonique interne : il est reconnu comme un poste interne et donc, dès qu'il est reconnecté à distance chez lui, son poste téléphonique à numéro interne redevient disponible. De plus, les appels qu'il peut alors passer seront véhiculés par l'entreprise, y compris vers l'extérieur ! De même, pour ses interlocuteurs distants, ceux-ci ont composé le numéro de poste interne ou externe standard et tomberont sur le bon interlocuteur, quel que soit l'endroit où il se trouve, à condition bien sûr qu'il ait démarré son système téléphonique IP et qu'il se soit connecté à l'entreprise par tous les moyens suffisants.

En conclusion, les besoins de mobilité peuvent être variés et adaptés à chaque situation (déplacements professionnels, maison, vacances, etc.). Il existe des réponses pour chaque besoin, certaines amenant plus de contraintes ou plus de facilité. De même, pour chaque besoin, différents types de matériel peuvent répondre plus ou moins bien, en tenant aussi compte des débits des connexions disponibles.

2. LES MATÉRIELS

Le choix du matériel dépend du besoin : à besoin précis, matériel approprié ; certains de ces matériels peuvent utiliser des liaisons sans-fil, qui seront détaillées dans le chapitre suivant.

2.1 – LE TÉLÉPHONE PORTABLE CLASSIQUE

Une simple version GSM n'offrira pratiquement aucune fonctionnalité, notamment due à la faiblesse du débit disponible ; dès que l'on passe au GPRS (suivant l'abonnement opérateur), le monde des données numériques s'ouvre et, si les fonctionnalités du téléphone sont là, on peut avoir accès d'une manière limitée à sa messagerie (mode IMAP, les derniers messages, pas de pièces jointes) ; le GPRS a un débit équivalent à un modem 56 Kbps.

Dès l'accès à la 2.5G (Edge) ou 3G (UMTS), les débits s'accélèrent mais les fonctionnalités du téléphone classique restent les mêmes, principalement du à la petitesse d'affichage ne permettant qu'une vingtaine de caractères et de la faiblesse des applications embarquées. La 3.5G (HSDPA) qui arrive permettra des débits encore supérieurs.

Pour la synchronisation des données personnelles, on pourra tout aussi bien utiliser les câbles fournis que l'infrarouge, ou mieux la liaison sans fil Bluetooth.

2.2 – LE SMARTPHONE

Là, le téléphone évolue en puissance et retrouve des logiciels embarqués plus puissants, ainsi qu'une résolution d'écran permettant une bonne lecture des messages, l'utilisation d'un navigateur classique Internet avec quand même une limitation de la partie visible d'une page web.

Souvent équipés GPRS/Edge, ils évoluent vers la 3G et bientôt 3.5G, donc vers des débits plus confortables, et certains y ajoutent la compatibilité Wi-Fi. L'écran est classiquement de type QVGA, soit 320x240, insuffisant pour de vraies applications bureautiques. La plupart du temps, on retrouve maintenant le logiciel Windows Mobile 5 pour Smartphone. La synchronisation des données se fera soit avec fil (USB) soit sans-fil avec des liaisons Bluetooth ou Wi-Fi.

2.3 – LE PDA

(Personal Digital Assistant ou Assistant Numérique Personnel, aussi appelé PocketPC)

De taille supérieure aux Smartphone, on retrouve ici sur les dernières générations des écrans de type large, avec une résolution de 640x480 VGA, devenant tout à fait viable pour la consultation des messages mais aussi pour la navigation Internet. L'utilisation de logiciels bureautiques devient envisageable, à

l'aide soit de l'écran tactile avec stylet et reconnaissance d'écriture manuscrite, soit grâce à un petit clavier virtuel ou réel. Ils sont souvent proposés avec le support Wi-Fi. Des deux mondes qui s'affrontaient, Palm Pilot et Microsoft, ce dernier semble avoir gagné avec l'évolution de son système PocketPC, re-baptisé Windows Mobile 5 dans les dernières générations.

Il est important de constater que des deux approches, PDA et Smartphone, il n'en restera bientôt qu'un, l'évolution de Microsoft étant vraisemblablement la fusion vers des PDA communicants, assurant le travail mixte de téléphonie et d'ordinateur. Reste à savoir si les progrès de la miniaturisation et la limitation de l'affichage sauront faire bon ménage ; tout le monde n'est pas prêt à transporter un PDA communicant de plusieurs centaines de grammes en permanence, et le porter à son oreille pour téléphoner (en revanche peut-être bien en le gardant à la ceinture et en utilisant une oreillette sans-fil).

2.4 – LE PC PORTABLE

Là, toutes les limitations précédemment évoquées sautent. Le prix à payer est le poids, l'encombrement, la plus faible autonomie, mais le confort d'un véritable écran et un grand clavier deviennent évidents. Les PC portables sont disponibles sous beaucoup de formats : on peut en envisager des puissants qui servent de machines principales au bureau et remplacent un PC fixe, ou bien encore des ultra-portables légers réservés aux déplacements. Il existe même des TabletPC à écran tactile pour ceux qui aiment cette approche. Un nouveau type de PC portable intermédiaire, l'UMPC (Ultra Mobile PC) est en train de voir le jour.

Ces PC sont souvent équipés de moyens de communication sans fil de type Wi-Fi, de modem analogiques classiques, mais peuvent être facilement dotés de fonctions téléphoniques par l'adjonction d'une carte GSM/GPRS/3G, la tendance actuelle étant d'intégrer ces moyens de téléphonie mobile directement dans les prochains PC.
Les grands acteurs comme Orange et SFR/Vodafone proposent de telles offres. Ainsi, avec de tels outils intégrant tous les moyens de communications actuels, la mobilité devient universelle, du moins tant qu'on se trouve proche de la zone de couverture de l'un des points ; on peut noter que les téléphones GSM/GPRS/3G modernes savent aussi communiquer sans-fil avec le PC par une liaison Bluetooth (le fil et l'infrarouge sont plus limités), et peuvent donc servir de moyens de communication si le PC n'est pas équipé de carte adéquate.

2.5 – LE TÉLÉPHONE IP

C'est aussi bien un logiciel qu'un matériel. Sous sa forme logicielle, il suffira de l'installer sur l'une des plates-formes compatibles (PC, PDA…). Skype en est un bon exemple. Mais il peut aussi se présenter sous forme matérielle : il est alors directement relié aux réseaux informatiques, soit par le fil, soit via un PC/USB, soit via le réseau sans-fil Wi-Fi. Certains constructeurs ont même conçu des téléphones mixtes, classiques et IP : on peut alors passer et recevoir des appels via le réseau classique mais aussi via IP. Si une solution comme Skype peut convenir aux particuliers ou à des petites structures, les entreprises qui veulent développer la téléphonie IP devront impérativement choisir les matériels et logiciels compatibles avec l'équipement central qu'ils ont choisi.

3. LES MOYENS DE COMMUNICATION ET LEURS DÉBITS

Avec ou sans fil, ils imposent les limitations de débit qui influencent directement la mobilité.

3.1 – LE FIL

Il sert aussi bien à relier un ordinateur au réseau que deux appareils entre eux pour par exemple une synchronisation.

3.1.1 – LE CÂBLE USB

Ce type de liaison sert surtout à synchroniser un téléphone portable ou PDA avec un PC ; câble de quelques mètres, il permet dans sa version 1 environ 1Mbps, et la version 2 actuelle offre des vitesses de l'ordre de 480 Mbps, autant dire aucune limitation pour synchroniser des données. Les socles de synchronisation livrés avec les PDA se connectent par ce biais-là (on fera juste attention au type de connecteur USB). Une évolution de l'USB vers le sans-fil (WUSB) est en cours, et permettrait des vitesses de l'ordre de 60 Mbps.

3.1.2 – LE CÂBLE ETHERNET

On reste ici principalement dans le monde de l'entreprise et pas dans le monde du nomadisme. Les vitesses sont conséquentes (100 Mbps à 1Gbps) et n'offrent pas de limitation pratique. Le nomade pourra éventuellement trouver ce type de liaison filaire dans deux cas : chez lui avec un modem/routeur ADSL ethernet style Freebox, mais aussi dans des hôtels ou centres de conférences disposant directement d'une liaison ethernet (le nomade avisé aura donc le câble Ethernet qui va bien avec lui).
Il est à noter que ce n'est pas parce que les débits Ethernet sont élevés que la liaison Internet derrière n'est pas limitée : par exemple la liaison Ethernet établie entre un PC et un modem ADSL peut être de 100 Mbps, mais le modem lui-même côté fil téléphonique sera par exemple limité à 4 Mbps (débit du fournisseur d'accès) ! C'est le tuyau le plus petit qui dictera sa loi et contraindra les outils à utiliser.

3.1.3 – LE MODEM TÉLÉPHONIQUE ANALOGIQUE

C'est l'ancêtre. On est connecté via une ligne téléphonique classique au débit de 56 Kbps maximum. Il y a peu à attendre de telles liaisons maintenant, mais elles peuvent rester un secours valable.

3.2 – LE SANS-FIL

3.2.1 – INFRAROUGE

La connexion infrarouge, lente et demandant aux deux matériels d'être proches et surtout face à face n'est pratiquement plus utilisée. Portée faible de quelques centimètres et débits limités au maximum à 115 Kbps, l'infrarouge est maintenant supplanté par les liaisons de type radio.

3.2.2 – BLUETOOTH

Il est rare d'utiliser ce type de liaison dans le cadre d'un réseau ; elle sera plutôt utilisée pour synchroniser des téléphones ou PDA à un PC. Le débit de l'ordre de 12 Mbps en version 1.1 et la portée de l'ordre de 10 mètres maximum. Bluetooth est plutôt l'apanage des accessoires de la téléphonie comme l'oreillette sans-fil, ou certaines imprimantes, mais les PC peuvent en être équipés. Un futur Bluetooth 2 est en préparation.

3.2.3 – LE WI-FI

Ce type de réseau sans-fil profitera aussi bien au nomade dans l'entreprise qu'en dehors. Concernant l'entreprise, on peut équiper des salles de réunion, des entrepôts en solution Wi-Fi. En dehors, ce type de réseau se trouve dans des hotspots, généralement accessibles dans les aéroports, hôtels et autres endroits publics. La portée est d'environ 100 m sans obstacle et la vitesse varie selon la norme : 11 Mbps en 802.11 b, 54 Mbps en 802.11 g ou a, voire plus avec des technologies propriétaires.
On notera cependant que ce débit est partagé entre tous les utilisateurs d'un point d'accès (AP = Access Point, une borne qui diffuse le signal avec son antenne) : plus il y a d'utilisateurs connectés simultanément, plus le débit est faible. Néanmoins, si la liaison qui se trouve derrière vers l'entreprise est suffisante, tous les types d'utilisation deviennent possibles. Ce type de connexion sans-fil s'est démocratisée, et il n'est pas rare de trouver des modems

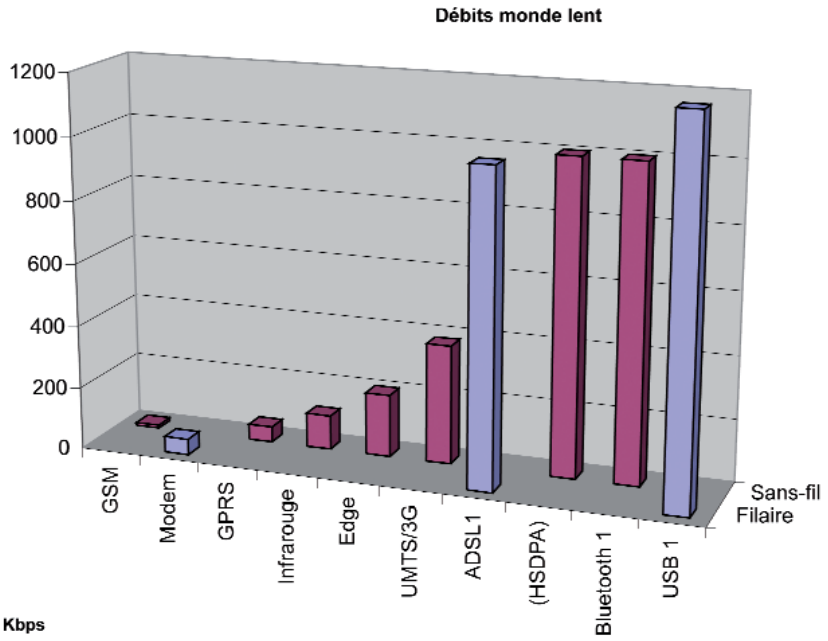
ADSL pour la maison équipés de Wi-Fi, ce qui permettra par exemple à un ordinateur proche d'être connecté avec câble ethernet au modem, pendant qu'un autre sera connecté sans-fil dans une autre pièce de la maison.
Les futures évolutions du Wi-Fi (MIMO/802.11n) et son probable successeur, le WiMAX, permettront des débits et des portées supérieures dépassant plusieurs kilomètres : déjà utilisés par certains opérateurs, ils devraient être accessibles aux utilisateurs finaux en 2007.

3.3 – LE RÉSEAU TÉLÉPHONIQUE GSM

C'est ici qu'on retrouve le gros des solutions de mobilité : dès que l'on est à portée d'un réseau GSM, on peut l'utiliser. Il s'agit d'abord d'avoir un abonnement, dont le prix et les fonctionnalités varient selon les opérateurs. En mode GSM simple, on est limité à des vitesses de l'ordre de 9600 bps, autant dire rien, si ce n'est un secours parfois appréciable pour consulter un ou deux messages.
En GPRS, on retrouve l'équivalent des modems filaires classiques, dans les 56 Kbps (Edge dans les 200 Kbps) ; là, on peut envisager la consultation de ses messages en se limitant sur les pièces jointes. En 3G/UMTS, les vitesses montent vers les 384 Kbits actuellement, ce qui correspond à un peu mieux que les premières connexions ADSL, mais la technologie évolue et les vitesses devraient aussi évoluer (HSDPA avec 1 Mbps). Avec la 3G et la future 3.5G, on ouvre la porte aux VPN, à l'accès à des ordinateurs distants et à la ToIP.

Schéma général des vitesses et débits de communication

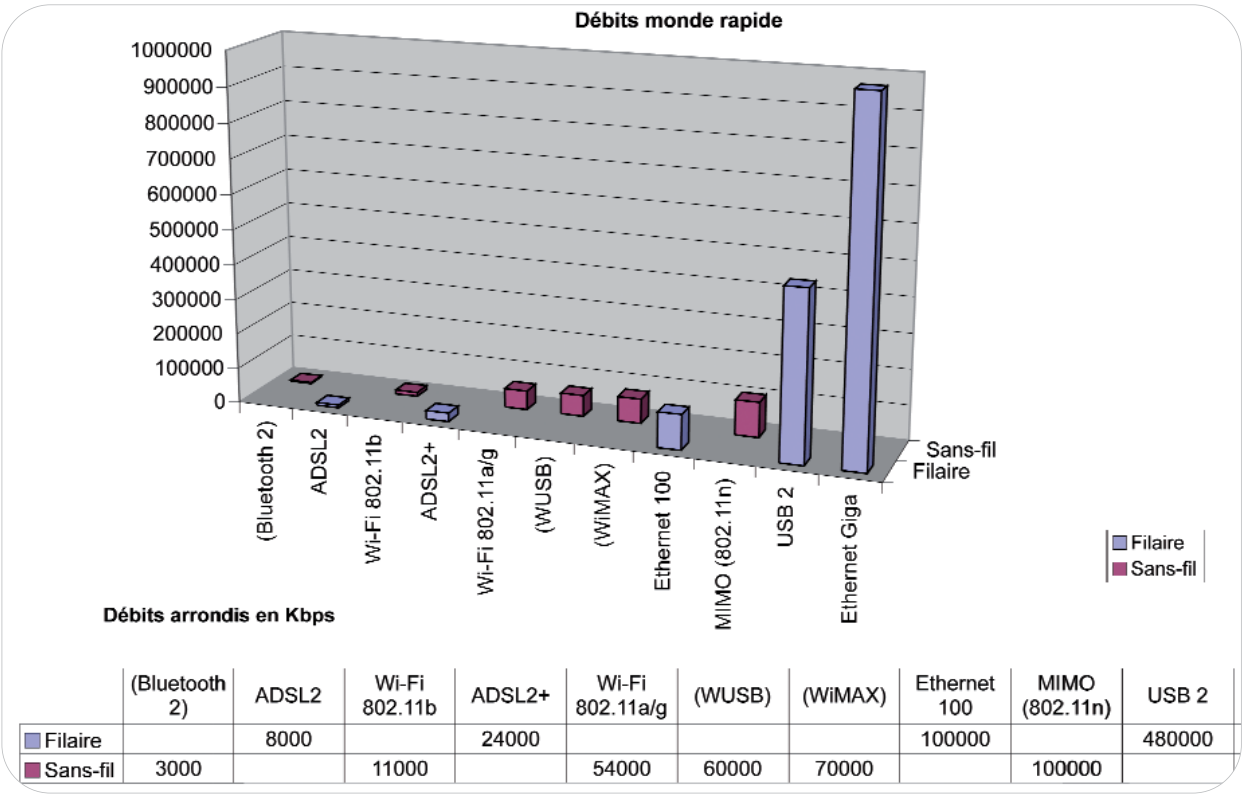
Monde lent (jusqu'à environ 1Mbps)



Débits arrondis en Kbps

	GSM	Modem	GPRS	Infrarouge	Edge	UMTS/3G	ADSL1	(HSDPA)	Bluetooth 1	USB 1
Filaire		50					1000			1200
Sans-fil	10		50	110	200	380		1000	1000	

Monde rapide



	(Bluetooth 2)	ADSL2	Wi-Fi 802.11b	ADSL2+	Wi-Fi 802.11a/g	(WUSB)	(WiMAX)	Ethernet 100	MIMO (802.11n)	USB 2
Filaire		8000		24000				100000		480000
Sans-fil	3000		11000		54000	60000	70000		100000	

Pour des raisons de lisibilité, l'échelle des chiffres présentés est en Kbps, arrondi aux milliers. Un caractère peut être grossièrement arrondi à 10 bits, ce qui peut donner le calcul suivant par exemple en GPRS :
50 Kbps = 50 000 bps = 5 000 caractères par seconde.
Ainsi, ce livre blanc avec les publicités pèse environ 5 Mo, ou encore 5 millions de caractères ; en GPRS à 5 000 caractères par seconde, il faudrait 1 000 secondes pour le récupérer, soit pratiquement 20 minutes !
NB : les technologies indiquées entre parenthèses sont en train de voir le jour et ne sont pas immédiatement disponibles.

4. CONCLUSION

En conclusion, il existe de nombreux matériels différents et des moyens de connexion avec ou sans fil variés, en constante évolution.
En mixant les bons matériels et les bonnes technologies de réseau, on peut répondre à toutes les problématiques du nomadisme : ce n'est qu'une réponse appropriée aux besoins exprimés, mais la réflexion doit être menée avec les professionnels de la mobilité et surtout de la sécurité.

PARTIE 2 – DROIT DU TRAVAIL ET NOUVELLES TECHNOLOGIES DE L'INFORMATION ET DE LA COMMUNICATION

La croissance des technologies de l'Information et de la Communication créée un bouleversement dans le monde du travail.

Elle modifie non seulement la physionomie des emplois mais également l'organisation du travail ainsi que les relations de travail.

La généralisation des technologies de l'information et de la communication a modifié le rapport du salarié à son outil de travail. Le travail dans un environnement informatisé fait appel à de nouvelles compétences et éloigne de plus en plus l'homme de "la chaîne de production" puisqu'il est amené à faire faire ce qu'il faisait auparavant par une machine qu'il programme. Ainsi les travaux, même dit d'exécution aujourd'hui, intègrent une part croissante d'initiative et de responsabilité.

De plus en plus de salariés qui utilisent l'informatique doivent exécuter non plus des tâches précises et standardisées mais sont tenus de réussir à atteindre des objectifs.

De nombreux emplois peuvent être remis en question, d'autres modifiés, l'automatisation de certaines tâches permettant de dégager du temps pour certains postes, ce même temps pouvant être utilisé à faire autre chose.

Un fossé peut se creuser parfois entre certains emplois et entre différentes générations de salariés.

Cet apport de technologie nécessite une capacité d'adaptation des salariés plus importante et crée des besoins en formation accrue.

Le développement faramineux en quelques années des NTIC a transformé aussi l'organisation même du travail en abolissant d'une part, la notion de distance et en modifiant d'autre part, le concept de temps. Or, la référence au lieu et au temps est aujourd'hui omniprésente dans notre droit du travail.

Ainsi, le droit du travail s'est construit dans le cadre d'un concept de l'entreprise définie en partie comme le lieu unique où se trouvent rassemblées toutes les ressources qui concourent à la production.

Or, l'informatique répond à un besoin de mobilité et permet ainsi de délocaliser des équipes de travail grâce au réseau intranet, la messagerie, l'agenda partagé, le groupware, mais permet également à un salarié de pouvoir travailler de chez lui tout en conservant un accès direct avec son environnement de travail par le moyen de technologies de l'information et d'outils de travail mobiles. Elle favorise et accentue le télétravail qui se développe aujourd'hui dans de nombreux secteurs d'activités et concerne de plus en plus toutes les catégories de salariés.

Ainsi, tout en conservant un poste de travail physique au sein de l'entreprise, le salarié peut utiliser les technologies de l'information et les outils de travail mobiles pour travailler depuis n'importe quel lieu. Ceci a comme incidence de "nomadiser" le travail de nombreux salariés, qui, jusque là étaient considérés comme ne pouvant exercer leurs fonctions que dans les locaux de l'entreprise.

Ces phénomènes de mobilité, encouragés ou accentués par les nouvelles technologies de l'information et de la communication, bouleversent de nombreuses notions admises jusqu'à présent.

Le fait de ne plus avoir de lieu de travail habituel ou d'en avoir un éloigné de l'entreprise, nous amène nécessairement à nous interroger sur le droit applicable, le type de couverture sociale, les formalités administratives à respecter.

Par ailleurs, la distance physique avec l'employeur peut modifier le lien de subordination et de dépendance du salarié. Les NTIC modifient les rapports hiérarchiques et peuvent conduire à une plus grande autonomie mais également parfois à une plus grande dépendance en raison de la multiplication des moyens les plus sophistiqués de pouvoir communiquer à tout moment et n'importe où (télé disponibilité parfois pesante).

Le travail peut ainsi s'immiscer dans les moindres interstices de la vie privée rendant difficilement appréhendable la notion de temps de travail effectif, (à savoir le contrôle de la durée du travail).

Les textes qui encadrent la mobilité du salarié sont plus ou moins importants dans le pays où l'on se trouve. Il faut savoir que le droit de l'Union Européenne fait grand cas de la mobilité des personnes et en premier lieu de celle des salariés. Pour favoriser cette mobilité, il s'est efforcé de créer les conditions propices à celle-ci d'une part, en orientant les membres de l'Union sur les règles du droit travail applicables mais également d'autre part, en prévoyant un accord sur le télétravail pour éviter l'insécurité juridique, conscient que le travail à distance se développe dans un cadre largement informel.

À Monaco, ce n'est pas encore le cas. Toutefois, il existe des textes qui encadrent certaines formes de mobilité. Ainsi, certains déplacements temporaires de personnels à l'étranger pour effectuer certaines missions provisoires, sont encadrés par des conventions bilatérales de Sécurité Sociale (Convention franco-monégasque de Sécurité Sociale signée en 1952 et Convention italo-monégasque de Sécurité Sociale de 1982, concernant les procédures de détachement). Par ailleurs, la Loi n°735 et l'Ordonnance 3217 encadrent le travail à domicile, de même la Loi n° 762 fixe le statut professionnel des voyageurs représentants, placiers.

Enfin, les grands principes du droit du travail s'appliquent, lesquels viendront limiter cette confusion des temps et des lieux et permettre de résoudre les conflits entre sources.

Toutefois, le droit devant constamment s'adapter, le télétravail offrant un certain nombre de potentialités : gain de productivité, gestion plus souple de l'emploi, diminution très significative des déplacements domicile-travail, diminution des surfaces de bureau, diminution co-relative des surfaces de parking, diminution de la consommation énergétique, nous serons certainement amenés à en rediscuter.

Ici, il est question d'être conscient des risques qu'entraînent les solutions de mobilité, sans pour autant avoir peur : il ne faut pas ignorer ces risques, il faut y répondre de manière appropriée et les réponses existent !
On dégagera deux aspects principaux : les dangers menaçant les utilisateurs mobiles, et ensuite nous parlerons des mesures à prendre.

1. LES DANGERS

1.1 – LES VIRUS, VERS, CHEVAUX DE TROIE, ET SPYWARE

Ces petits programmes malveillants sont capables de détruire des données et de se propager : la réponse classique est d'utiliser un programme anti-virus. Il est peu probable de trouver un PC moderne non équipé d'antivirus ; en entreprise, il se mettra à jour d'une manière centralisée, ce qui pose un premier problème : comment se mettra-t-il à jour une fois que le nomade sort de l'entreprise ? Les éditeurs d'antivirus ont les solutions, encore faut-il penser à les mettre en œuvre. Et si pour quelque raison que ce soit un poste n'était pas mis à jour, il pourrait revenir dans l'entreprise ou s'y connecter à distance et introduire alors un virus : il existe des solutions de contrôle qui sont capables de vérifier si un poste est à jour avant qu'il ne se connecte à distance ou au moment où il revient en entreprise.
Mais trouve-t-on des virus dans les plus petits (PDA, téléphones) ? Oui, certains commencent à être découverts, et bien sûr les éditeurs de solutions antivirus commencent à offrir des antivirus pour les PDA et les téléphones GSM.

1.2 – LES ATTAQUES DIRECTES

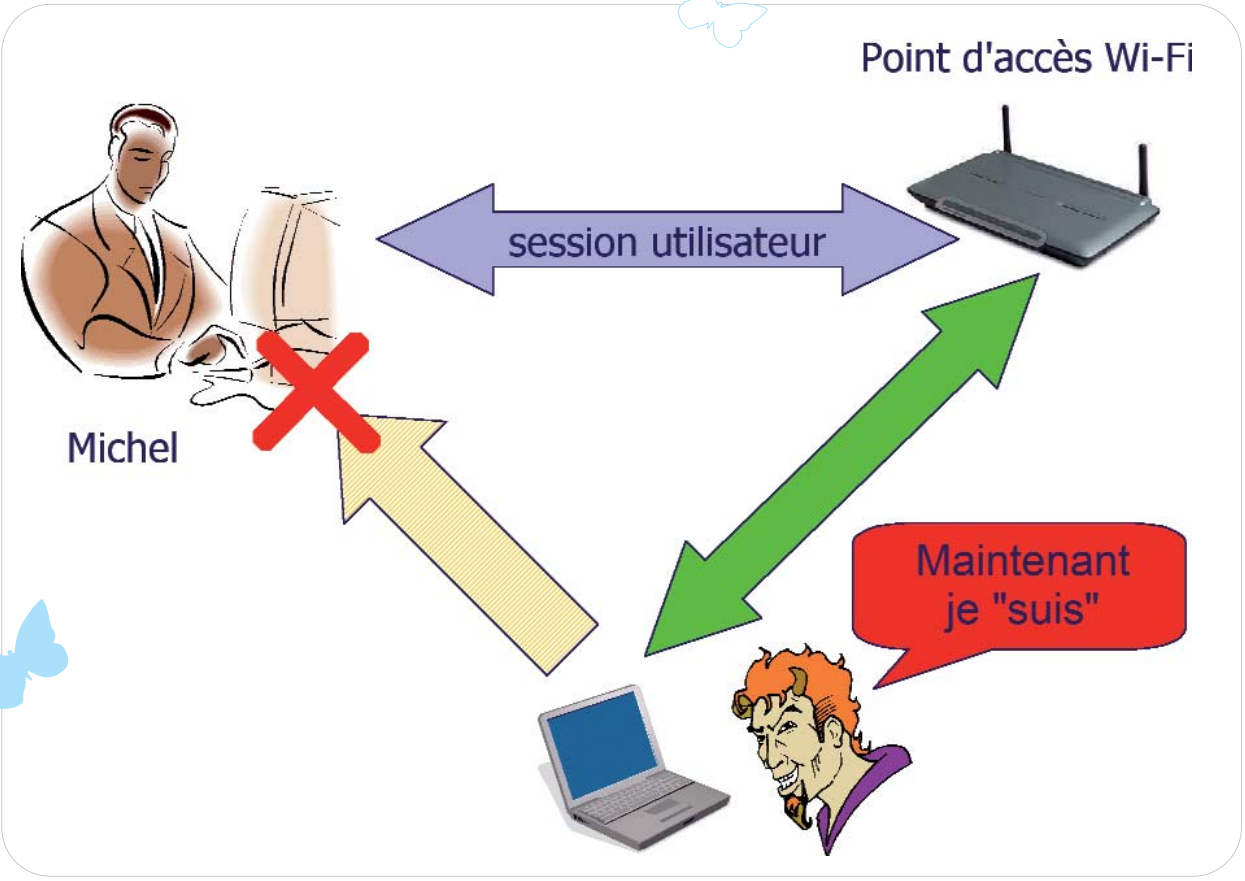
Toutes les entreprises connectées à Internet sont maintenant sensibilisées : elles se sont équipées de firewall et autres systèmes de prévention d'intrusion. Les ordinateurs de l'entreprise sont donc bien protégés de l'extérieur.
Mais alors qu'en est-il des nomades ? La même problématique se pose : dès que le nomade établit connexion (typiquement Internet), il se retrouve exposé aux mêmes menaces que son entreprise : il doit donc être équipé d'un firewall qui le protégera de l'extérieur. Du plus simple au plus sophistiqué qui vérifiera chaque programme dans la machine, c'est un point de passage obligé. Les grands éditeurs offrent des solutions pour administrer à distance et en temps réel les firewall équipant les utilisateurs nomades.

1.3 – LE PHISHING

Le phishing est une nouvelle menace qui s'étend : de faux site Web voient le jour, qui ressemblent comme deux gouttes d'eau à leurs originaux. Par exemple, un simple message reçu vous avertit que vos coordonnées bancaires doivent être mises à jour et vous invite à aller sur le site de votre banque : vous tapez en confiance votre nom et votre mot de passe, mais malheureusement, c'est à un pirate que vous êtes en train de les envoyer.

1.4 – LE DÉTOURNEMENT DE SESSION

Technique utilisée en environnement Wi-Fi, le détournement de session consiste à mettre momentanément hors service l'ordinateur d'un utilisateur (par plantage, généralement) puis la personne malveillante continue la session en se faisant passer pour l'utilisateur en question.



1.5 – LE WARDRIVING

Pratique de plus en plus répandue où le pirate potentiel sillonne les rues d'une ville pour répertorier et cartographier les divers points d'accès Wi-Fi ainsi que les informations permettant de s'y connecter. Le pirate va ensuite publier toutes ces informations sur Internet.

2. PARADES ET MESURES À PRENDRE

1.1 – MAINTENANCE ET ATTITUDE PRÉVENTIVE

Lorsqu'on parle de sécurité, il est fondamental d'avoir une attitude proactive. Que ce soit pour un ordinateur portable ou un PDA, il ne faut pas négliger les sauvegardes. Il faut aussi régulièrement tester celles-ci et mettre en place un plan de récupération après incident… de préférence avant l'incident. Le système d'exploitation et les applications doivent être mises à jour régulièrement car de nouvelles failles de sécurité sont constamment découvertes et permettraient à un virus ou un pirate d'endommager le système. Il est très important dans l'entreprise de mettre en place des systèmes de détection d'intrusion (IDS - Intrusion Detection System), car certaines entreprises ne se rendent même pas compte qu'elles ont été victimes d'attaques et d'intrusions. Seule une audit de sécurité sérieuse et approfondie, peut révéler ce genre de problème.

1.2 – STOCKER DES DONNÉES ENCRYPTÉES

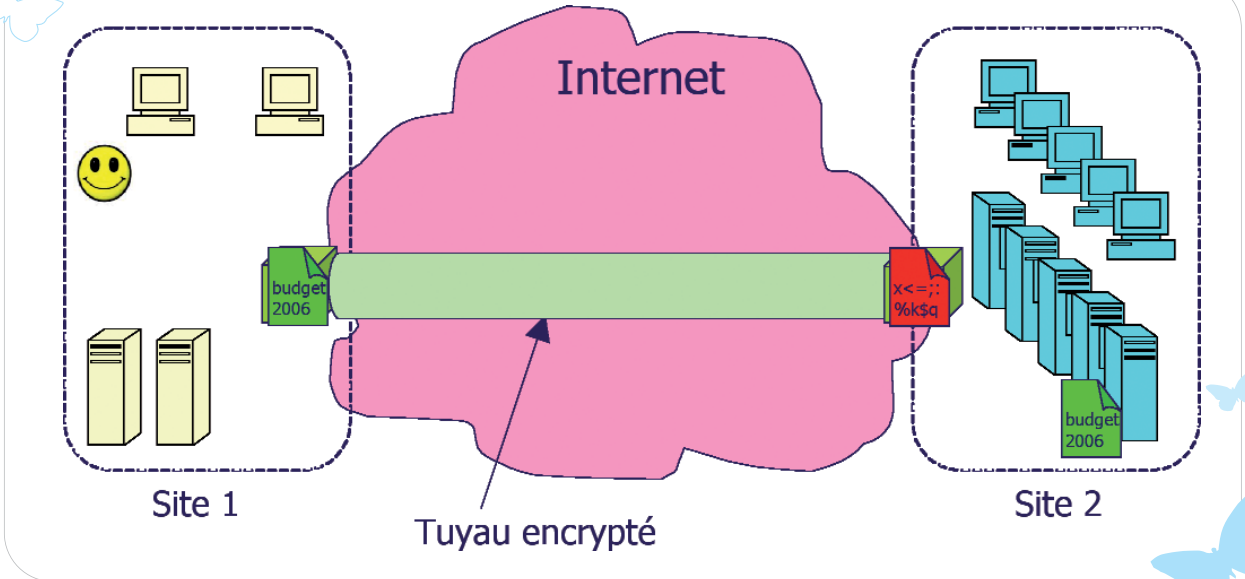
Que se passerait-il si son appareil nomade était perdu ou volé ? Ce qui arrive malheureusement fréquemment. Sans protection adéquate, toutes les données stockées deviendraient alors disponibles à des tiers plus ou moins bien intentionnés. Et ne croyez pas que le mot de passe de démarrage Windows les arrêtera bien longtemps !
La solution est là bien évidemment de crypter/chiffrer les données sur le disque dur, sur le PDA et sur tout autre dispositif de stockage (p. ex. clé USB). On peut envisager des solutions légères qui consistent à ne chiffrer que les documents sensibles, ou des solutions plus lourdes qui chiffrent la totalité du disque. Certains constructeurs proposent même des systèmes intégrés à des PC portables.

1.3 – SSL ET HTTPS

Derrière l'abréviation SSL (Secure Sockets Layer), se cache un protocole complexe que pourtant des millions de personnes utilisent dans le monde, souvent sans le savoir ; il s'avère extrêmement résistant.
Si vous vous êtes déjà connecté à votre banque via Internet ou avez déjà effectué des achats sur Internet, vous avez déjà dû voir une petite fenêtre s'afficher vous avertissant que vous allez passer en mode sécurisé juste après, l'adresse Internet que vous avez tapée se transforme alors en acheter "https" : vous faites alors du SSL, c'est-à-dire que les données désormais échangées sur Internet sont cryptées/chiffrées et qu'un pirate ne peut rien en tirer.
Si vous vous connectez à distance à votre entreprise, soit pour accéder à un site Web Internet/Intranet ou à votre messagerie/agenda/carnet d'adresses en mode navigateur Web, la seule mise en place d'une connexion SSL vous assurera la confidentialité. Ce que l'on sait moins, c'est qu'avec les clients de messagerie classique non Web, comme par exemple Microsoft Outlook, il est aussi possible de mettre en œuvre SSL (en smtp, pop3 et imap) pour envoyer et recevoir ses messages en mode sécurisé : personne ne pourra lire les messages s'ils étaient interceptés.

1.4 – LE RÉSEAU PRIVÉ VIRTUEL - VPN

Pour les besoins qui nécessitent plus qu'un simple navigateur ou client de messagerie, par exemple l'accès à des documents du réseau, à des applications spécifiques ou à des sessions à distance, il devient nécessaire d'établir un réseau privé virtuel/VPN avec l'entreprise. Ce tuyau ainsi établi à distance, qui permet de passer tous types d'informations entre le réseau d'entreprise et le nomade doit aussi rester confidentiel.
Quel que soit le type de VPN mis en œuvre, les données échangées sont alors cryptées/chiffrées et deviennent incompréhensibles à d'éventuels espions.



1.5 – PROTECTION DES RÉSEAUX SANS-FIL

Mettre en place un point d'accès Wi-Fi est la portée de nombreuses personnes. Les matériels disponibles sont tellement "intelligents" de nos jours qu'il n'est pas trop difficile de les faire fonctionner. Il ne faut cependant pas oublier de mettre en œuvre l'authentification (donner son nom et son mot de passe) et plus important encore, activer le cryptage de la communication. Divers protocoles de cryptage existent. Un des premiers d'entre eux s'appelle WEP (Wired Equivalent Privacy). Il est facile à mettre en œuvre, mais ne fournit pas une excellente protection (il est tout à fait décodable). On trouve sur Internet des logiciels gratuits permettant de décoder du WEP, moyennant simplement… un peu de temps et de patience. Il faut donc aujourd'hui mettre en œuvre des protocoles de protection plus sérieux, de type WPA (Wi-Fi Protected Access) et WPA2 (encore meilleur).

1.6 – L'AUTHENTIFICATION

La question qui se pose ici est : qui est là ?

Se connecter à distance à une messagerie ou un réseau d'entreprise n'est pas sans danger, et on a intérêt à être sûr de l'identité de celui qui se présente. Actuellement, l'immense majorité des authentifications sont faites par couple login/mot de passe : si l'on peut s'en contenter localement ou dans le cadre de machines personnelles, l'absence de sécurité de cette solution entraîne de gros risques professionnels. Les mots de passe sont généralement choisis de manière simpliste, trop courts, évidents comme le prénom de la femme, des enfants, date de naissance, voiture, chien, etc., voir simplement notés dans un carnet d'adresses ou sur un post-it collé sous un clavier. Toute personne devinant le mot de passe à alors accès à toutes les données de la personne ainsi piratée !

Et ceci sans parler des systèmes à découverte de mot de passe par force brute qui peuvent tester des milliers de combinaisons possibles pour finalement trouver la bonne, si toutefois on n'a pas prévu de limiter le nombre de tentatives avant de bloquer.

Ne parlons pas non plus de cette nouvelle génération de logiciels espions/key-logger qui s'installent sur une machine et qui savent espionner toute frappe clavier y compris celle des mots de passe.

Il existe heureusement autre chose que le simple mot de passe !

L'authentification forte fait appel à trois facteurs :
1 > ce que l'on sait : ça, c'est le classique mot de passe,
2 > ce que l'on possède : un dispositif spécial, comme une carte à puce, une clé USB, une calculatrice à mot de passe aléatoire, un certificat numérique X.509,
3 > ce que l'on est : un élément physique comme l'empreinte d'un doigt, la forme d'une main, d'un visage, c'est la biométrie,
et il faut allier au moins deux de ces trois facteurs !

Par exemple, quand vous retirez de l'argent à un distributeur, vous utilisez deux facteurs :
1 > ce que l'on sait : votre code PIN,
2 > ce que l'on possède : votre carte bancaire à puce ; l'un sans l'autre ne mène à rien.

1.7 – LA FORMATION

Un certain nombre de problèmes de sécurité sont liés à un manque de formation des utilisateurs. En effet le matériel et les logiciels disponibles de nos jours sont généralement très puissants et offrent de nombreuses fonctionnalités (très souvent même beaucoup trop). Il n'est pas rare de rencontrer des personnes qui à cause d'un manque de formation, mettent en danger les données informatiques qui deviennent alors très vulnérables.

Après cette revue de besoins, moyens de connectivité et solutions, y compris avec les évolutions constantes en cours, il devient évident que le nomade moderne trouvera toutes les réponses à ses besoins : si les réponses n'existent pas tout de suite, soyez sûr qu'elles ne tarderont pas à venir.

Autonome ou conseillé et installé par un professionnel, le nomade devra toujours garder en ligne de mire que sa mobilité entraîne des risques supplémentaires à ne pas ignorer.

QUELQUES TERMES TECHNIQUES ET ABRÉVIATIONS

2.5G/3G/3.5G > G pour les différentes Générations en téléphonie mobile.

Bluetooth > Connexion sans-fil limitée pour petits périphériques, issue de la téléphonie.

Edge > Evolution du GPRS en 2.5G, peu utilisée par rapport à la 3G.

GPRS > General Packet Radio Service, réseau de données sur GSM.

GSM > Global System for Mobile Communications, le réseau téléphonique portable actuel.

HSPDA > High Speed Packet Data Access, évolution suivante de l'UMTS en 3.5G.

UMTS > Universal Mobile Telecommunications System, évolution 3G de la téléphonie data.

802.11* > Normes IEEE pour les réseaux sans-fil, on y trouve le Wi-Fi 802.11a/b/g.

802.16 > Normes IEEE pour les réseaux sans-fil de type WiMAX.

AP > Access Point, point d'accès/borne réseau sans-fil.

https > Hyper Text Transfer Protocol Secure sockets : protocole de navigation web sécurisé.

IMAP > Internet Message Access Protocol, protocole permettant de lire et synchroniser sa messagerie à distance.

PDA > Personal Digital Assistant, petit ordinateur portable léger.

PocketPC > autre nom du PDA.

Pop3 > Post Office Protocol 3, protocole pour récupérer sa messagerie.

Pushmail > système de messagerie qui "pousse" les messages vers l'utilisateur sans qu'il ait à venir les chercher.

RPV > Réseau Privé Virtuel, voir VPN.

Smartphone > Téléphone intelligent, avec des fonctions de PC.

SSL > Secure Sockets Layer, protocole de sécurisation de données, notamment utilisé sur le web avec "https".

TabletPC > PC équipé d'un grand écran tactile et d'un stylet, reconnaissance d'écriture manuscrite.

UMPC > Ultra-Mobile Personal Computer, PC entre le PDA et le portable, avec écran tactile et stylet.

USB > liaison avec fil pour périphériques PC.

VPN > Virtuel Private Network (RPV en français), établir un réseau privé sécurisé avec son entreprise en traversant un réseau non sécurisé type Internet.

WEP > Wired Equivalent Privacy : solution de sécurité Wi-Fi, maintenant dépassée par WPA.

Wi-Fi > Wireless Fidelity, autre nom des réseaux sans-fil de type Ethernet.

WiMAX > Worldwide Interoperability for Microwave Access, évolution du Wi-Fi.

Windows Mobile > Système d'exploitation de Microsoft pour PDA et Smartphone.

WPA > Wi-Fi Protected Access, évolution de la sécurité Wi-Fi, succédant au WEP.

WUSB > Wireless USB, évolution sans-fil de la norme USB.

REVUE DE **PRESSE**

JDN solutions

En 2006, convergence et mobilité guideront les choix des DSI

Comment les DSI doivent-ils aborder cette nouvelle année ? Les conseils du cabinet Gartner renvoient à des technologies qui deviendront certainement incontournables en 2006. (04/01/2006)

Le cabinet Gartner Group définit une série de recommandations à destinations des DSI pour l'année à venir. Derrière les conseils formulés par les analystes Mark Raskino et John Mahoney, un inévitable rapprochement entre les utilisateurs et les technologies ayant fait leurs preuves en 2005 pointe son nez.

Alors que les choix de 2005 tournaient davantage autour des politiques de réduction des coûts ou de croissance (*lire **l'article** du 21/12/2004*), le cabinet préconise une modernisation nécessaire des politiques d'usage et d'exploitation du système d'exploitation pour 2006. Parmi la foulée de conseils, cinq grands axes s'inscrivent plus particulièrement dans la stratégie de développement des entreprises sur le plan technologique.

1/ Repenser l'usage des logiciels internes

L'usage d'un logiciel - et même encore plus d'un progiciel - ne doit plus se concevoir comme l'achat d'une licence par poste client pour une utilisation souvent assez maigre des fonctionnalités du produit. C'est pourquoi le modèle technologique du "Software as a Service" (SaaS) est à étudier pour une migration intelligente des usages applicatifs spécifiques.

Louer un service dématérialisé sur un serveur dédié apporte de nombreux avantages, en plus d'une souplesse dans l'admnistration et un coût optimisé, donc réduit. Les précurseurs de ce modèle - Webex, Salesforce et Google - ont été suivis par des géants tels IBM et Microsoft. Le langage XML facilite le développement de services ainsi hébergés.

2/ Rendre convergentes les technologies de la communication

Depuis les théories de Shannon et Weaver, la communication dans les organisations n'est pas exempte de défauts. L'harmonisation des technologies peut pourtant accroître la productivé des équipes, tout en diminuant les côuts.

Pour répondre à cette problématique, une stratégie tout IP semble adaptée. Grâce au Multi Protocol Label Switching (MPLS) il est ainsi possible de rassembler sur un seul protocole la voix téléphonique, l'interconnexion de serveurs, les réseaux ATM, l'accès Internet, des passerelles et un VPN.

3/ Accompagner les échanges entre sites distants

La convergence IP ne se résume plus au seul réseau interne. Dans toute organisation moderne, la mobilité fait partie du quotidien. C'est pourquoi la norme Wimax - et son concurrent sud-coréen WiBro - sont d'ores et déjà perçus comme les meilleurs moyens d'accès à des VPN sécurisés *via* un réseau très haut débit, de l'ordre de 70 Mbps.

Avec une portée théorique de 50 km, il deviendra très aisé de déployer un réseau entre plusieurs sites ou d'ouvrir un réseau pour un partage des ressources.

4/ Optimiser le développement d'applications mobiles

Les terminaux mobiles ne se cantonent plus à de simples communications téléphoniques. Les *smartphones* devraient même - à terme - remplacer les PDA car la convergence est l'un des premiers critères de choix. Dès lors, les applications doivent suivre cette tendance et s'installer sur ces outils nomades.

Au vu des capacités et du succès des terminaux Blackberry ou des modèles Nokia tournant sous Symbian OS, la synchronisation entre le mobile et l'ordinateur portable appartiendra bientôt au passé car des applications professionnelles - comme pour la finance et la gestion de projets - utiliseront directement les nouveaux réseaux rapides pour échanger leurs données avec le serveur central de l'entreprise.

5/ Tirer profit de l'évolution d'Internet

Cette étape passe bien évidemment par la formation des collaborateurs aux nouveaux usages d'Internet. Derrière l'évolution du réseau - l'Internet 2.0 en regroupe les améliorations - les flux RSS, les weblogs, les réseaux sociaux et le langage client Ajax doivent devenir des références pour tous, de l'utilisateur au développeur.

Le commerce en ligne sait d'ailleurs bien associer toutes ces nouveautés pour conquérir de nouveaux clients séduits tant par l'aspect fonctionnel du site que par sa base produits, où le moteur développé suivant le langage Ajax facilite l'interaction entre les requètes du navigateur client et le serveur, le tout en XML.

Ainsi, force est de constater le rôle toujours plus présent de la convergence et de la mobilité. Une organisation performante devra rapidement se mettre au gout du jour pour étendre sa productivité n'importe où, avec des outils connectés au SI central. Ceci passe aussi par un développement encore plus personnalisé des applications, tenant compte de ces usages mobiles et du mode hébergé.

■ Christophe COMMEAU, JDN Solutions

MOBILITÉ WINDOWS ET SYMBIAN SONT LES SYSTÈMES VEDETTES DES PC DE POCHE

Des terminaux prêts pour la convergence fixe-mobile

La frontière devient de plus en plus floue entre le monde des smartphones et celui des assistants personnels. La généralisation des puces GSM ou GPRS intégrées et la téléphonie sur Internet pourraient achever cette convergence.

GPRS ou WiFi? Les deux! C'est ce que proposent désormais quelques constructeurs avec des terminaux de poche capables de se connecter aussi bien aux réseaux mobiles des opérateurs qu'aux points d'accès publics ou des entreprises. L'intérêt pour ce type de produits est récent. Le M600 d'Eten date de décembre dernier et les modèles de Sony Ericsson et de Nokia ne sont même pas encore disponibles. En outre, beaucoup de fournisseurs manquent à l'appel. Pas question pour autant de parler de retard technologique des uns ou des autres. Il semble qu'il s'agisse d'un choix assumé. La demande de terminaux GPRS (ou 3G) et WiFi reste assez faible, notamment parce que l'Internet sans fil est très consommateur en énergie par rapport aux connexions GPRS ou 3G. Pour les utilisateurs nomades qui se contentent d'envoyer des courriels et de naviguer un peu sur le Web, les gains en débits des réseaux sans fil ne compensent donc pas toujours les pertes en termes d'autonomie. Pas davantage pour les techniciens qui s'appuient sur des applications optimisées et peu consommatrices de bande passante. Parmi les constructeurs, le canadien RIM, qui fournit le Blackberry, ne propose ainsi aucune solution GPRS WiFi en France, bien que le produit existe et soit disponible outre-Atlantique. Les opérateurs mobiles français ne lui ont pas demandé.

Besoin de plus d'autonomie

Cela évoluera-t-il dans les mois qui viennent? Sans doute. « *On a déjà fait de gros progrès. Dans le monde du mobile et l'autonomie est évidemment une priorité*, explique Émilie Jourdran, chef de produits E-series chez Nokia. *Nous avons fait une première expérience WiFi avec le 9500. Pour les nouveaux modèles, nous avons optimisé l'appareil et avons mis une batterie en conséquence.* » « *On peut toujours débrayer la fonction WiFi si besoin* », ajoute Fabrice Côme, chef de produits chez Partelec, distributeur en France des produits Eten.

Au-delà de l'autonomie, c'est l'intérêt même de la double connexion qui doit être étudié. Pour réellement décoller, ce type d'offres aura sans doute besoin de la voix sur IP. Grâce à des logiciels de téléphonie sur Internet comme Skype

Neuf terminaux de poche pour réseau mobile ou local




Constructeur / Modèle	Fujitsu Siemens Pocket Loox 700	Nokia E61	Nokia E70	Eten M600
Système d'exploitation	Windows Mobile 2003 SE	Symbian OS v. 9.1	Symbian OS v. 9.1	Windows Mobile 5.0
Écran	3,6 pouces, 640 x 480 pixels	240 x 320 pixels	352 x 416 pixels	2,8 pouces, 320 x 240 pixels
Processeur	520 MHz (Intel)	non communiqué	non communiqué	400 MHz (Samsung)
Mémoire	128 Mo	75 Mo	75 Mo	128 Mo
Edge	non	oui	oui	non
UMTS	non	oui	oui	non
WiFi	802.11b	802.11g	802.11g	802.11b
Bluetooth	oui	non	oui	oui
Appareil photo	1,3 mégapixel	non	2 mégapixels	1,3 mégapixel
ToIP	non	SIP	SIP	Skype
Taille	122 x 72 x 16,1 mm	117 x 69,7 x 14 mm	117 x 53 x 22 mm	111,7 x 60,7 x 22 mm
Poids	170 g	144 g	124 g	165 g
Prix	710 € HT	400 € HT	435 € HT	500 € HT

ou à des clients SIP, la voix sur WiFi pourrait permettre aux utilisateurs de téléphoner gratuitement lorsqu'ils sont connectés à un point d'accès sans fil. Mais attention. Premièrement, les abonnés qui peuvent choisir la voix sur IP sont ceux qui souscrivent à des forfaits données et qui utilisent donc par ailleurs des applications mobiles. Sauf que la plupart préfèrent aujourd'hui avoir deux terminaux distincts (un pour les données et un pour la voix) plutôt que cumuler les fonctions sur un équipement qui n'est finalement approprié à aucune des deux utilisations. «*Nous avons, à un moment, proposé une carte GPRS pour la voix sur notre assistant personnel*», se rappelle Antoine Ferraz, chef de produits des solutions mobiles chez Fujitsu Siemens. Avant d'expliquer que la demande n'a pas suivi. Deuxièmement, les grands opérateurs mobiles ne veulent pas aujourd'hui de voix sur IP sur leurs réseaux : pas plus au travers de leurs points d'accès publics WiFi que sur leur réseau mobile (*voir encadré*). Troisièmement, les connexions aux *hotspots* restent très chères aujourd'hui. Si on dépense en WiFi ce que l'on économise en téléphonie mobile, il n'y a plus guère d'intérêt.

Pas de voix sur IP sur les réseaux mobiles

Comparant parfois la troisième génération de téléphonie mobile à une espèce d'ADSL sans fil, les opérateurs mobiles ne veulent pourtant pas entendre parler à ce jour de voix sur IP sur leurs réseaux de données. La culture de la quasi-gratuité n'est pas encore celle de SFR, d'Orange ou de Bouygues, qui se doivent de rentabiliser leur infrastructure et qui comptent sur la commercialisation de leurs forfaits voix pour y arriver.

Un avantage pour les opérateurs purement WiFi, qui, eux, peuvent se permettre d'ouvrir leurs réseaux à la voix. Peut-être aussi un avantage pour les futurs opérateurs Wimax. Il y a près d'un an, Altitude Télécom inaugurait le premier réseau de ToIP par boucle locale radio sur l'autoroute A28. Mais pour espérer une généralisation, il faudra d'abord que les terminaux intègrent ce nouveau protocole de communication.

Appels gratuits avec le WiFi

Reste en revanche la possibilité de téléphoner gratuitement depuis les sites de son entreprise équipés de bornes d'accès ou des halls d'accueil de sociétés partenaires, par exemple. Les points d'accès publics y sont de plus en plus présents. Le logiciel Skype est aujourd'hui intégré au M600, mais il peut aussi être installé par les utilisateurs sur la plupart des terminaux. Le plus avancé des fournisseurs sur le sujet est peut-être Nokia, qui intègre un client SIP à ses produits et qui, grâce à des partenariats avec Avaya et Cisco, devrait proposer dès le mois prochain une vraie itinérance entre les réseaux mobiles et WiFi et donc, une vraie convergence fixe mobile. Dès qu'il entrera dans son entreprise, l'utilisateur devrait pouvoir se servir indifféremment de son portable et de son fixe, l'autocommutateur étant capable de capter les appels et de s'affranchir des réseaux mobiles pour router les communications des téléphones mobiles WiFi. Or on sait que les appels passés depuis un mobile à l'intérieur de l'entreprise sont très nombreux. Parmi les produits répertoriés dans le tableau ci-dessous, ceux de Qtek et de Eten sont animés par la dernière mouture du système d'exploitation mobile de Microsoft, Windows Mobile 5.0. Celui-ci intègre davantage qu'auparavant la problématique de la double connexion GPRS WiFi. Il permet au terminal de repérer les deux types de réseaux et demande à l'utilisateur lequel il doit choisir dès lors qu'il avoisine un point d'accès sans fil. Windows Mobile 2003 SE ne possédait pas cette fonction. Pour le reste, tous les terminaux intègrent les principales applications bureautiques. Ils se distinguent essentiellement par leur ergonomie et la présence ou non de claviers et de connectivités Edge ou UMTS. Chez Fujitsu Siemens, l'option GPRS (pour les données uniquement) est proposée au sein d'une carte d'extension CompactFlash. Chez Sony-Ericsson et Nokia, les terminaux sont très orientés courriels. Outre les compatibilités Blackberry, ActiveSync (solution Microsoft) ou Visto, le finlandais intègre évidemment sa récente technologie Nokia Business Center.

OLIVIER DESCAMPS

 Qtek Qtek 2020i	 Qtek Qtek 9000	 Qtek Qtek 9100	 Sony Ericsson P990i	 HP iPAQ hw6900
Windows Mobile 2003 SE	Windows Mobile 5.0	Windows Mobile 5.0	Symbian OS 9.1	Windows Mobile 5.0
3,5 pouces, 320 x 240 pixels	3,6 pouces, 640 x 480 pixels	2,8 pouces, 320 x 240 pixels	2,8 pouces, 320 x 240 pixels	3 pouces
520 MHz (Intel)	520 MHz (Intel)	200 MHz (Texas Instruments)	non communiqué	416 MHz (Intel)
128 Mo	128 Mo	128 Mo	80 Mo	64 Mo
non	non	oui	non	oui
non	oui	non	oui	non
802.11b	802.11b	802.11g	802.11b	802.11b
oui	oui	oui	oui	oui
1,3 mégapixel	1,3 mégapixel	1,3 mégapixel	2 mégapixels	1,3 mégapixel
non	non	non	non	non
130 x 69,9 x 18,2 mm	127,7 x 81 x 25 mm	108 x 58 x 23,7 mm	114 x 57 x 25 mm	118 x 71 x 18 mm
190 g	285 g	160 g	150 g	179 g
670 € HT	1 050 € HT	630 € HT	non communiqué	610 € HT

VoIP et téléphonie sur Internet

Quels risques de sécurité pour l'entreprise ?

PDA, smartphones, PC portables, travailleurs distants, hotspots, workspots... les moyens et les canaux d'accès au système d'accès de l'entreprise se multiplient. Comment dès lors éviter les virus, les hackers, les erreurs et les actes de malveillance ?

La VoIP offre, selon ses défenseurs, deux avantages : une réduction des coûts de télécommunication et le développement de nouveaux usages, rendus possibles grâce au protocole IP. Or si l'on n'y prend pas garde, ces atouts peuvent fondre comme neige au soleil. *« Aujourd'hui, la première préoccupation d'une entreprise est* « quel impact aura sur mon budget la migration vers la VoIP ». *La sécurité n'est pas encore un point important de ses préoccupations. Or il s'agit d'un problème majeur, car la VoIP hérite des risques liés au monde IP »*, estime Alain Dagois, responsable des opérations chez l'organisme de formation Global Knowledge France. A cela, il faut encore ajouter les risques hérités de la téléphonie classique. La mise en place d'une solution de VoIP ne doit donc pas se faire les yeux fermés. D'autant que l'investissement nécessaire pour sécuriser l'application peut réduire à néant les gains financiers escomptés. Cette protection doit prendre en compte trois chaînons vulnérables : le réseau, les serveurs et passerelles, ainsi que les terminaux. *« Il faut protéger l'IPBX contre les atteintes à son intégrité, mettre à l'abri les applications voix comme la messagerie, empêcher l'écoute du site ou intersite, éviter les fraudes qui consistent notamment à utiliser l'entreprise comme relais pour des communications illicites, interdire l'utilisation de logiciels incontrôlés à la Skype, qui bypassent le système téléphonique de l'entreprise, et prendre en compte la qualité de service »*, énumère Etienne Coulon, VP Marketing & Business Development, d'Arkoon qui propose des appliances de sécurité VoIP.

Tout le monde se penche sur le problème

Bien sûr, tous les acteurs du marché se sont attelés au problème, notamment les constructeurs. *« On peut compter sur eux pour proposer des offres de plus en plus intégrées, avec notamment des firewalls inclus dans le call server »*, croit savoir Pierre Anne, expert technique chez l'intégrateur Ineo Com. *« La sécurisation de la VoIP est soumise aux mêmes contraintes que les autres applications IP, toutefois, en terme de processus, ces dernières ne sont pas transposables. Les appels ne sont pas prédictibles, on ne sait pas qui va communiquer avec qui et pendant combien de temps. Une connexion à une banque de données est par exemple plus longue et plus lisse qu'une communication téléphonique. D'autre part, la sécurisation souhaitée par le client risque d'augmenter le temps de latence, de dégrader la voix. C'est un vrai challenge auquel nous nous sommes attelés »*, rappelle toutefois Philippe Cuningham, spécialiste sécurité de Cisco France.

PHILIPPE CUNINGHAM - Cisco france

« La sécurisation de la VoIP est soumise aux mêmes contraintes que les autres applications IP, toutefois en terme de processus, ces dernières ne sont pas transposables. Les appels ne sont pas prédicitibles »

Chez Avaya on tente d'éviter les attaques en utilisant un OS Linux renforcé et en séparant les flux, de manière telle que le téléphone n'accède jamais au serveur. 3Com propose quant à lui en option une sonde Tipping Point qui analyse les flux voix et data. Chez les opérateurs aussi on affirme prendre le maximum de précautions. France Télécom a ainsi créé une division ad hoc rattachée directement à Didier Lombard. *« La voix passe par un réseau MPLS inaccessible par Internet. Nous maîtrisons l'origine des flux et leur qualité de service. Nous vérifions par exemple que l'adresse d'où vient l'appel est réservée à la VoIP. Nous distinguons également signalisation et voix. Ces procédures s'appliquent également à la visioconférence, la seule différence concerne le dimensionnement des accès »*, affirme Jean-Pascal Jullien, directeur des Services Communications Multimédia chez FT. Bien entendu, les spécialistes de la sécurité s'intéressent également à ce marché en pleine expansion. Thales propose ainsi le chiffrement du PABX et des passerelles, couplé à une sonde intégrée au téléphone.

retenir une solution qui s'intégrait à notre ancien système téléphonique, notamment pour pouvoir réutiliser nos téléphones analogiques. Enfin pour la mobilité, la solution DECT proposée par Philips nous a convaincu », explique-t-il. En effet, la solution de Philips permet par exemple de pouvoir transférer facilement les appels d'un téléphone portable vers un téléphone mobile DECT, mais aussi d'envoyer des SMS. L'opéra a notamment utilisé cette possibilité d'envoyer et de recevoir des SMS pour connecter son installation téléphonique à son système d'alarme incendie. Ainsi, lors d'un incendie, tous les employés sont automatiquement prévenus via l'envoi de SMS d'alerte sur les téléphones DECT.

Plus de 80 % des tickets

sont vendus via le centre d'appels.

Des services pratiques avant tout

Mais la mobilité n'est pas le seul atout de la solution Philips. Les deux PABX IPS2000 installés au siège de l'opéra à Göteborg et à Skövde ont pu être reliés via un lien IP, mais également via deux liaisons E1. « *En cas de problème sur le réseau IP nous pouvons émettre et recevoir des appels via notre centre d'appels. En effet, dans ce centre les trois opérateurs utilisent des téléphones IP pour une meilleure intégration au serveur de centre de contacts. C'est très important, car plus de 80 % de nos tickets sont vendus via notre centre d'appels. Nous ne pouvons pas accepter une interruption de service* » précise le directeur technique.

Enfin, la solution Philips était compatible avec le serveur de présence Intercept Messaging 80/20, une solution développée par une société suédoise. Ce serveur très pratique permet de connaître la disponibilité en temps réel de chaque employé et de gérer des renvois d'appels sur les téléphones DECT ou d'envoyer des SMS d'état (en réunion, en voyage...). «*L'année prochaine, nous allons intégrer notre solution téléphonique à nos badges d'entrée-sortie pour savoir automatiquement lors d'un appel si un employé est dans le bâtiment ou en dehors des locaux* » se félicite Maths G. Nyström.

Au final, en prenant en compte ces fonctionnalités et le coût de la solution Philips, très concurrentiel par rapport aux solutions tout IP, l'opéra est très satisfait de son choix. Parfois, il vaut mieux choisir des solutions pragmatiques plutôt que d'aller vers une course à la technologie, vers le tout IP. C'est le message qu'a voulu nous faire passer l'opéra de Göteborg, fidèle au pragmatisme à la suédoise.

ALAIN COFFRE

Technology

IDENTITY CRISIS

TARGETING INSTITUTIONS...

Most people who fall victim to identity theft never meet the culprits. Recent high-profile thefts have hit big institutions, but everything from giant data-brokerage firms to tiny local bank branches is a potential target.

WHO ELSE HAS IT

Why the recent rise in major heists? Blame it on the "third party" players, who now have more access to financial information and related data than ever before. Here are some favorite places where ID thieves go to get the goods:

- > Banks, schools, employers and doctors
- > Government agencies
- > Phone companies
- > Merchants
- > Card networks
- > Credit-reference agencies
- > Data-brokerage firms
- > Payment-processing agencies

YOUR DATA

Your real fingerprints aren't etched on your fingertips; they're stored on computers and printed on paper and plastic. What ID thieves want:

- > Credit-card numbers
- > CW2 security numbers (on back of credit card)
- > Credit reports
- > Social insurance numbers
- > Driver's license numbers
- > *ATM cards*
- > Telephone calling cards
- > Mortgage details
- > Date of birth
- > Passwords/PINs
- > Home address
- > Phone numbers

HOW IT'S STOLEN

Security is lax and identity crooks are cunning. Some recent cases:

HACKING

DSW: In April, the shoe chain revealed that hackers had stolen data from 1.4 million credit- and debit-card transactions at 108 stores in the U.S. The breach also included account numbers from 96,000 check transactions.

Exposed: 1.5 million

CardSystems: This U.S.-based data processor improperly held on to credit-card info for "research." Among those exposed: cardholders in Japan, Hong Kong, the Philippines and Australia.

Exposed: 40 million

CONS AND SCAMS

MphasiS/Citibank: Employees of an Indian outsourcing firm allegedly conned help-line callers into divulging personal data that the thieves used to drain the callers' Citibank accounts.

Stolen: $350,000

Sumitomo Bank: A gang used key-logging software to steal passwords and access the network. They were busted just prior to making off with:

$397 million

...AND YOU, TOO

Stealing wallets is *so* 1995. Today, identity thieves rely on a variety of tactics (both high- and low-tech) to pick your pocket. A look at the most popular—and effective:

'Shoulder surfing': Lurking at ATMs or phone booths to pick off PINs, credit-card numbers or passwords.

'Skimming': Stealing credit- or debit-card numbers by attaching a data-storage device to an ATM or the card reader at a retail checkout terminal.

Dumpster diving: Rifling through trash bins—home, office, public—for loan applications, credit-card documents and any printed identification numbers.

'Phishing/pretexting': Posing by e-mail or phone as a legit company and claiming there's a problem with your account.

SOURCES: FEDERAL TRADE COMMISSION, PRIVACY RIGHTS CLEARINGHOUSE AND CONSUMER SENTINEL

ILLUSTRATION BY VIKTOR KOEN FOR NEWSWEEK

Tough privacy laws help protect many people in Europe, but elsewhere, identities are a hot commodity. Fifty million Americans have recently had data exposed, and a quarter of Britons know someone whose identity has been stolen. Here's how thieves do it.

LACK OF CARE

Citibank: The May disappearance of a UPS shipment of customer data tapes in the U.S. eerily echoes a similar theft last year in Singapore; 123,690 Japanese bank customers had their data records vanish during shipment between offices.

Exposed: 3.9 million

BANK BLUNDERS

Aozora Bank: Clients of the Kyoto, Sapporo and Shibuya branches in Japan had personal info exposed when microfilm data were lost in March.

Exposed: 26,400

Commonwealth Bank of Australia: In March, a rogue manager used client IDs to access ATMs and transfer cash between banks to feed his gambling addiction. He confessed.

Stolen: $17 million

Central Bank of Russia: Confidential info on bank transfers of settlements was reportedly sold online in April.

Michinoku Bank: In April, this Japanese bank mistakenly threw out three CDs containing the backup copies of the financial records of nearly its entire customer base.

Exposed: 1.3 million

HOW IT'S USED

Whether they find it in a stolen wallet or buy it from a shady Internet trader, with enough information, criminals can assume an identity and quickly commit a flurry of costly crimes. The estimated annual tab: $53 billion in the U.S.

Credit cards: Some charge to an existing account; most create new ones. Thanks to new safeguards, this category has been trending down since 2002.

Phone/utilities: 16% of all ID-fraud complaints mention opening new phone accounts; 5% mention utilities charges.

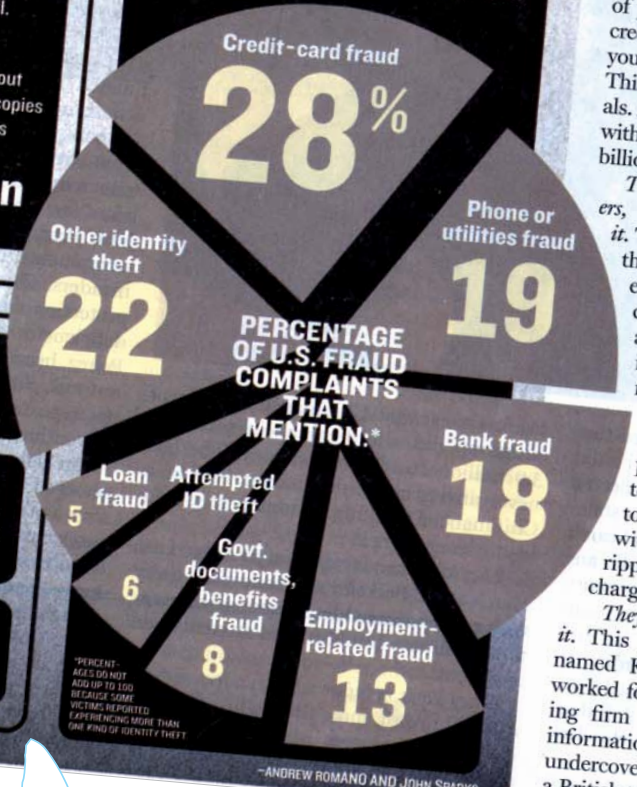
Banks: Twice as many draw from (and drain) existing accounts as create new ones; fraudulent electronic-fund transfer has doubled since 2002.

Employment: Using stolen name and identity to get hired; up 4% in the past three years.

Government: Bogus ID cards and driver's licenses; tax fraud; stealing benefits.

Loans: Mostly business, personal or student loans; also auto loans/leases and mortgages.

Other: Using stolen identification when caught committing a crime; also insurance and securities fraud, health-care scams and bankruptcy schemes.



'Social engineering': Pretending to be a landlord, loan officer or employer in order to access your info.

Mail theft: Mining mailboxes for new credit cards, preapproved credit offers, insurance statements, tax info, benefits documents and investment reports.

'Retail' theft: Stealing files, hacking into records or conning/bribing workers at local retail stores or medical offices.

—ANDREW ROMANO AND JOHN SPARKS

swipes not just your card but also your entire financial persona. Judy McDonough, a 56-year-old occupational psychologist from the north of England, has been living a nightmare since last year, when she found that someone—she suspects a relative—racked up £33,000 of debt over three years, which included two credit cards, three bank loans and £2,300 of catalog orders. She reported the crime six times before taking it to her member of Parliament. Most banks, says McDonough, "just hope you'll go away."

For years, the primary cause of ID theft has been good old-fashioned analog crime. Thieves rifle mailboxes, snatch purses and dive into the garbage for discarded bank statements or credit-card receipts. More recently, we've seen a plague of "phishing"—sending bogus e-mails that look as if they come from legitimate companies, asking us to supply personal information. After the CardSystems heist, phishers, trying to capitalize on the news, sent out e-mails supposedly from MasterCard, asking people to update their information. "They played on the fear that consumers had when the announcement was made," says Susan Larson of SurfControl, an Internet-security firm.

Savvy computer users know the requisite defense against a phishing attack: never respond to a request for personal information. This wisdom is part of the standard tool kit of protections against ID theft. Check your credit-card bills with an eagle eye. Request your credit report. Shred your information. This regime makes perfect sense for individuals. But when it comes to companies charged with safeguarding millions, sometimes even billions, of records, what do they do?

They leave it unencrypted on computers, where malicious hackers get hold of it. The DSW Shoe Warehouse is far from the only hacked database owner. According to a U.S. government consent order, BJ's Wholesale Club, a Massachusetts-based firm operating big-box stores and gas stations, not only failed to encrypt, but stored records in violation of bank-security rules, didn't use a firewall to prevent wireless intrusions and protected the information with the easy-to-guess default passwords that came with the system. Result: credit cards ripped off in early 2004 were used to charge millions in goods.

They inadvertently allow employees to sell it. This June, a 24-year-old Indian man named Karan Bahree, who at the time worked for Gurgaon-based online marketing firm Infinity eSearch, allegedly sold information on 1,000 bank accounts to an undercover journalist working for The Sun, a British tabloid, for £2,750, according to a

COMPUTER SECURITY

NASTY, BRUTISH, AND SNEAKY

Hackers have raised the stakes with a new bug almost immune to detection

BY BRIAN GROW

AS A DATA SECURITY specialist, Jeremy Pickett sees all kinds of digital tricks. So on Mar. 20, when he was tracing the origins of a computer worm that had been blocked the night before from entering a client's computer network, Pickett wasn't too surprised that it tried to connect with four sleazy Web sites, most of them, he believes, in Russia. Or that it then tried to load victims' PCs with as many as 30 new pieces of "malware," ranging from spam programs to those that automatically dial in to expensive phone-sex services.

But the real shock came when Pickett decided to test another bug by infecting his own PC with it. Out slithered a program that promptly installed itself deep inside his computer. There it became virtually immune to detection from the basic antivirus software that scans for dangerous code. The bug—known as a "Trojan," which in turn was hidden inside a "rootkit"—was designed to activate whenever a Web surfer typed in a user name or password for bank accounts or Web sites for dating, social networking, or e-mail. Pickett went to a bank site and entered fictitious log-in information. Right before his eyes, those data were sent streaming back to Russia, joining the IDs of thousands of real victims. His reaction: "absolute horror."

This nasty bit of code, appropriately named "the Hearse" by Pickett's employer, Sana Security Inc. in San Mateo, Calif., is threatening to raise the stakes in the spy-vs.-spy war over cybercrime. That's because the average computer security program sifts for known worms and viruses on PCs. But rootkits cloak data-stealing code so that it can hide in the deepest guts of Windows software without showing up in task lists as an active program. Criminals, having greatly expanded their knowledge of Windows' inner workings, are flocking to this new tool. Russian computer security company Kaspersky Lab estimates that on average 28 new rootkits emerged each month in 2005, up from six per month in 2004.

Only five of 24 antivirus outfits picked up the Hearse outbreak by Mar. 21, according to virus tracker VirusTotal.com. At first, antivirus giant Symantec Corp. was not among them, though it says it detected the bug the next day. In one of the first real-time cyber stakeouts, Sana monitored one of the Russian Web sites for four days in late March. Ironically, it was left open to public view thanks to a security lapse by its unknown operators. Pickett watched as some 90,000 pieces of personal data from clients of more than 6,500 companies flowed across his screen. "It's like [Pickett] put on night vision goggles and watched," says John M. Frazzini, CEO of Secure Systems Corp. and former head of the Secret Service's Electronic Crimes Task Force in Washington. The show lasted until a Russian Web host, warned by Sana, took the site down on Mar. 24.

Equally alarming is the roster of victims, a cross-section of American business. Customer accounts for companies such as social networking site MySpace.com, auction site eBay Inc., credit-card and banking company Capital One Financial Corp., and Internet service provider AOL Inc. were compromised, *BusinessWeek* learned. Names and passwords from over 2,000 MySpace accounts were stolen. Spokeswoman Dani Dudeck says the company "takes user privacy and site security very seriously and quickly responds to all potential threats."

Many companies, though menaced anew every day, still don't have systems in place to react quickly to warnings. When Pickett and co-workers contacted some of them, they received automated e-mail responses or had to call multiple people. One unnamed company reported Sana officials to its nuisance department. Some moved faster. EBay quickly blocked compromised accounts until new passwords could be set. Bank of America Corp. officials immediately contacted the Secret Service's Criminal Investigative Div.

And the Hearse? Analysts suspect the hackers simply moved to a new, undetected collection spot. Warns Sana CEO John Zicker: "How deep does the rabbit hole go? Did we get there? No." ■

What a Scam

The Hearse outbreak allowed thieves to steal user names, passwords, and bank accounts. The toll:

90,000	37,000	6,500
Pieces of personal data stolen	Online accounts compromised	Companies hit

Data: *BusinessWeek*

ALEX NABAUM

GROUPE

ASCOMA

Courtage d'Assurances et de Réassurances

www.ascoma.com

ASCOMA
24 bd Princesse Charlotte
98000 Monaco
Tel +377 97 97 22 04
Fax +377 97 97 22 05
E-mail : info@ascoma.com

cybersquatting ?

phishing ?

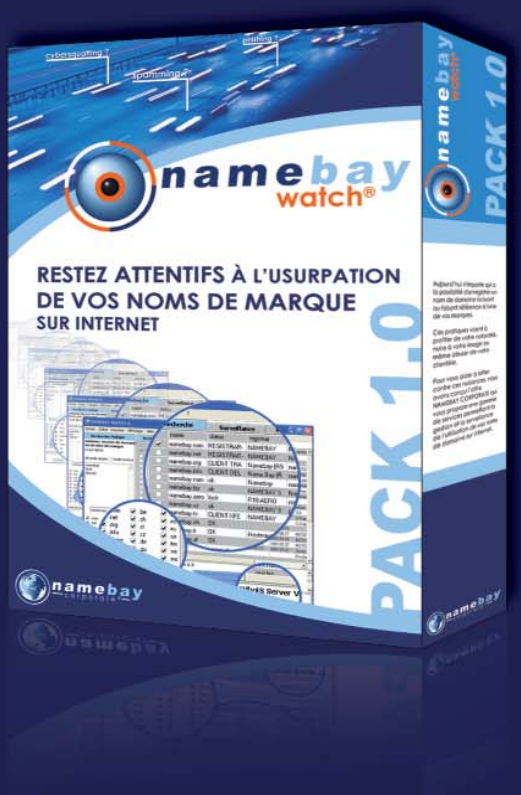
spamming ?

namebay corporate®

votre bureau d'enregistrement de noms de domaine
spécialisé dans la protection de vos noms de marque

services d'assistance personnalisés

dans le réglement des litiges
sur les noms de domaine



solution puissante et performante

de lutte contre les nuisances
sur internet
(surveillance de marques,
gestion des noms de domaine, ...)

CONTACTEZ-NOUS

NAMEBAY - Service Corporate - 27 Bd des Moulins MC98000 MONACO
email : commercial@namebaycorp.com - http://www.namebaycorp.com

Laisseriez-vous cet individu fouiller dans les données de votre entreprise?

Check Point Integrity vous protège des logiciels espions.

Check Point Integrity™, solution leader au plan mondial pour la sécurité des postes de travail, protège les entreprises de tout préjudice financier causé par des individus de ce genre lorsque des logiciels espions (spyware) s'infiltrent dans vos réseaux par des voies dérobées, volent ou divulguent des données sensibles, dégradent les performances de vos PCs et augmentent les dépenses de support technique.

Outre la neutralisation des logiciels espions, Integrity apporte à l'ensemble des postes et des réseaux une protection complète et éprouvée contre les vers les plus récents et les toutes nouvelles techniques d'intrusion.

Les moyens de défense préventive d'Integrity comprennent le firewall personnel universellement reconnu comme le plus fiable, le blocage des menaces régulièrement annoncées, les préventions d'intrusion, l'éradication des logiciels espions. Vous avez ainsi la certitude que seuls des PCs sains sont autorisés à se connecter aux réseaux. Facile à déployer et administrer, Integrity, plus que n'importe quelle autre solution, s'adapte à un grand nombre d'outils réseaux et fournit une protection absolue à tous vos accès.

Avec Integrity vous pouvez dire adieu aux logiciels espions et… à ce genre d'individus.

Pour en savoir plus sur les logiciels espions et sur Integrity, visitez le site www.checkpoint.com où vous pouvez télécharger le White Paper Neutralizing Spyware in the Enterprise Environment.

Check Point
SOFTWARE TECHNOLOGIES LTD.
We Secure the Internet.

NOVENCI

Intégrateur de Technologies dans le domaine de la mobilité

Conçues en fonction de chaque profil constituant le personnel d'une entreprise, NOVENCI propose un panel de solutions où la technologie se met au service des besoins fonctionnels de chaque utilisateur mobile.

Le pôle de compétence EIS, Expertise en Infrastructure et Sécurité

maîtrise les technologies de mobilité, d'optimisation et d'évolution de vos infrastructures data et conçoit une solution globale composée des éléments indispensable de votre architecture étendue :

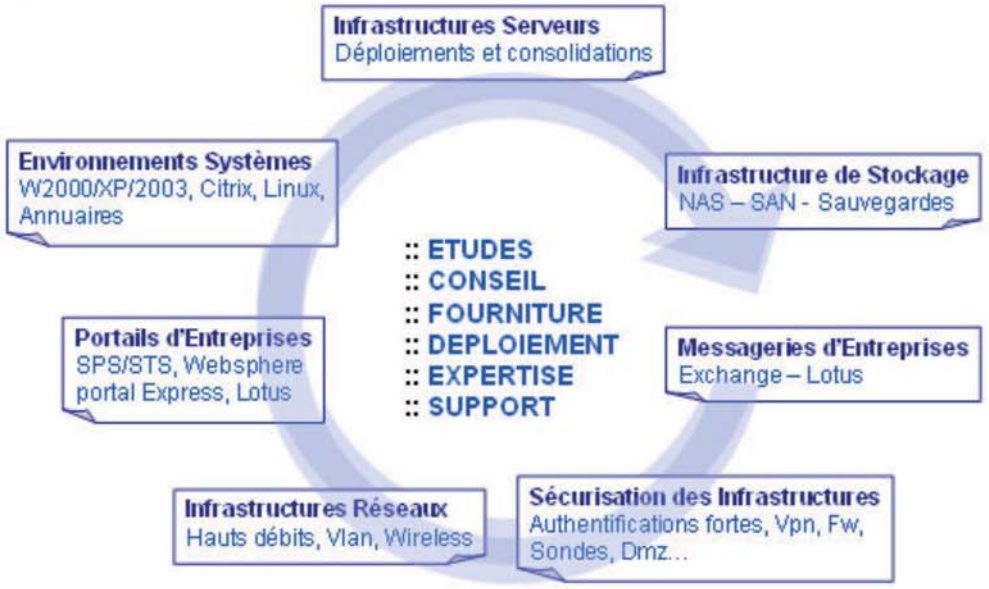
- Analyse de portabilité de vos applications au modèle d'accès distant
- Design de l'architecture centralisée
- Modèle de sécurité
- Conseil et choix sur l'opérateur DATA
- Conseil et choix sur le terminal d'accès idéal (PC portable, PDA, Smartphone…)

Son expérience vous permettra de disposer d'une vision globale intégrant les aspects de sécurisation, de choix de matériel et de déploiement.

La standardisation et la mutualisation des infrastructures IP constituent un gisement de diminution des coûts, qui passe par des choix pertinents.

Pour vous accompagner, Novenci vous propose une prise de contact avec ces technologies via «l'analyse d'opportunité Mobilité dans l'entreprise étendue».

Le Pôle Ingénierie & Solutions Infrastructures



www.novenci.com

2006 Preferred Partner* *Partenaire Privilège

hp invent

IBM Business Partner

Lotus software

Microsoft GOLD CERTIFIED Partner

CITRIX access PARTNER SILVER Solution Advisor

2 Boulevard Rainier III - 2ème entresol ouest - MC 98000 MONACO
Tél. : 00.377.99.99.69.99 – Fax : 00.377.99.99.69.98

AVOLYS

Centre de formation informatique Monégasque

AVOLYS, le Meilleur de la formation dans le domaine des Nouvelles Technologies :

Une offre complète

✓ **Filière Utilisateur**	Bureautique, Publication Web et Internet Dessins, Photos, Infographie
✓ **Filière technique**	Systèmes & Réseaux, Langages et Développement Bases de Données, Sécurité, Wifi Travail Collaboratif, Portail
✓ **Filière Méthodes et Organisation**	ITIL, Gestion de projet

Des solutions de formation à la carte

INGENIERIE DE FORMATION

✓ **Audit/Diagnostic**
Mesure des écarts de compétences par rapport aux objectifs

✓ **Préconisations**
Définition des formules pédagogiques les mieux adaptées par rapport au profil des stagiaires et à leurs objectifs

✓ **Bilan pédagogique**
Evaluation de la qualité
Mesure de l'efficacité de la formation
Reporting et Certifications
Solution post formation

DIFFERENTES FORMULES DE FORMATION

- ✓ Formations présentielles inter/intra
- ✓ Ateliers thématiques
- ✓ Formule Centre de ressources
- ✓ E learning
- ✓ Coaching

www.avolys.com

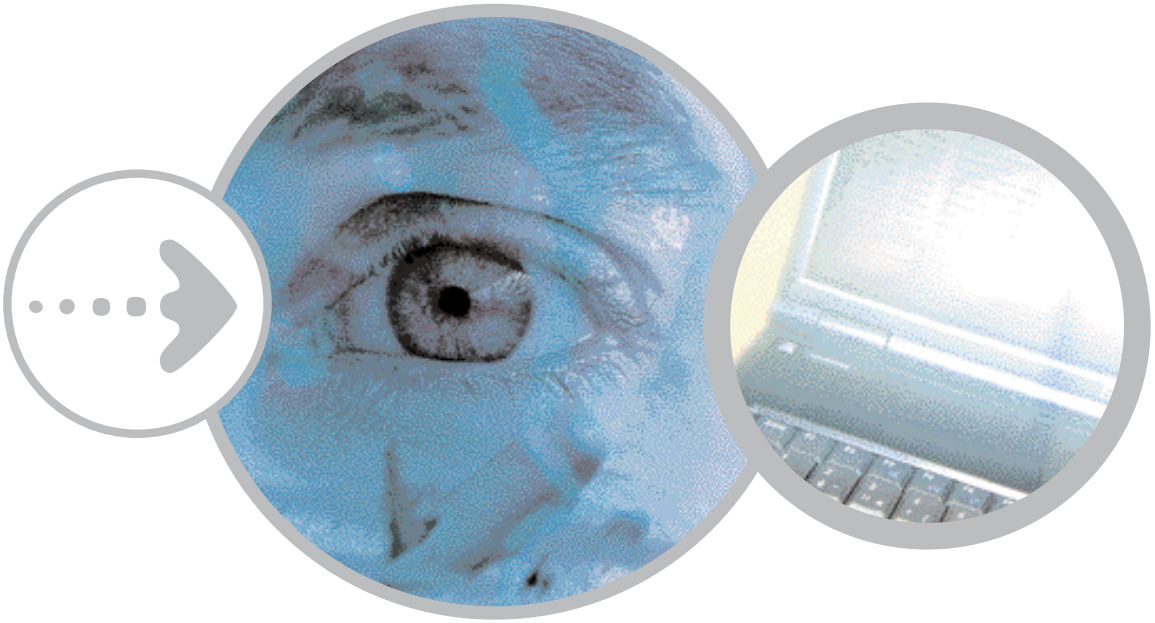
2 Boulevard Rainier III - 2ème entresol ouest - MC 98000 MONACO
Tél. : 00.377.99.99.69.99 – Fax : 00.377.99.99.69.98

TEKWORLD
GROUPE MICROTEK

> Managers Worldwide Mobile Access (IPass, WeRoam)

> **E-vision** : Entreprise WLAN, VPN Security Solutions & WIFI solutions, IP plateform "VOIP"

> **Activ Portal** : Net Platform allowing CRM, Portal, Workflow, Reporting, Billing, Customized Applications



Ou contactez-nous :
TEKWORLD
2, boulevard Rainier III
MC 98000 Monaco
Tél. +377 93 10 42 82
Fax +377 93 10 42 83
e-mail : info@tekworld.mc

TEKWORLD
GROUPE Microtek