



### MAGAZINE

Intranet-Extranet  
DSI  
Systèmes-Réseaux  
Sécurité  
Développement  
Emploi, RH  
CRM-Marketing  
e-PME

SITES WEB  
Séminaires

### ACTUALITES

Acteurs  
Télécoms-FAI  
Mobile  
Actu High Tech  
Actu économique

Bref France  
Bref International

CAC 40 **-0.22%**  
CAC IT20 **+0.54%**  
Nasdaq **-0.30%**  
Dow Jones **+0.01%**

JDN Finance

### TOUS NOS ARTICLES

Dossiers  
Enquêtes  
Interviews  
Cas d'entreprise  
Analyses

Juin  
Mai  
Avril  
Et avant

Emploicenter

Cherchez une offre

### ANALYSE

[Sommaire Sécurité](#)

## 10 conseils pour sécuriser son parc mobile

**Smartphones, PDA communicants, ordinateurs portables, périphériques externes : la mobilité se développe en entreprise mais elle implique une plus grande exposition aux risques de sécurité. 10 conseils pour y faire face.** (09/06/2005)

Le concept d'entreprise étendue séduit visiblement de plus en plus les professionnels. Au premier trimestre 2005, les ventes de smartphones et PDA communicants ont progressé de 82% en volume selon le cabinet d'études Canalys. Une évolution suivie par le lancement des services de téléphonie de troisième génération (*lire l'article du 30/11/2004*) et le développement des points d'accès publics pour réseaux sans fil.

[10 conseils pour mettre en place un réseau local sans fil](#)

[Dossier](#) [Mobilité](#)

### QUIZZ ANTI-STRESS

**DANS QUELLE ENTREPRISE STRESSE-T-ON LE PLUS ?**

Parallèlement, les ventes d'ordinateurs portables sur l'ensemble du territoire français ont décollé de 24,3% en volume pendant l'année 2004, selon le spécialiste Gartner. En comparaison, la croissance française des ventes d'ordinateurs sur l'année 2004 s'élevait à 17,7%. Les progrès technologiques ont largement favorisé cet essor. Actuellement, un PDA dispose d'un microprocesseur aussi puissant que ceux des ordinateurs vendus trois ans plus tôt.

Des progrès qui ont également porté sur la densité de stockage et les médias amovibles. Désormais, les clefs USB disposent d'un espace disque de plusieurs gigaoctets, facilitant le transport d'informations. Reste que ces technologies comportent de sérieux risques en matière de sécurité qui ne peuvent être toujours résolus. Il convient dès lors de bien justifier l'usage de la mobilité et d'en encadrer le fonctionnement.

### 1) Chiffrer le contenu des terminaux mobiles

Que ce soit le smart phone ou l'ordinateur portable, les terminaux mobiles contiennent des informations sensibles appartenant à l'entreprise qui sortent

**TREMIC**

Ne laissez pas le spyware voler votre pro

[>> Téléchargez](#)

### Newsletters

- Solutions [Voir un exemple](#)
- Journal du Net [Voir un exemple](#)
- Emploi [Voir un exemple](#)
- Développeurs [Voir un exemple](#)
- Evénements et Etudes Benchmark [Voir un exemple](#)

[Toutes nos newsletters](#)

### EVENEMENT **Petit déjeuner NOHET COFIDIS**

"Grâce à la gestion de contenu 300 Call Center traitent efficacement jus quotidiens" - M. Devos, CdP Intranet

du périmètre de sécurité traditionnel. En cas de vol ou de perte, un terminal non crypté facilite grandement la tâche du nouveau propriétaire de l'appareil. Une mesure de cryptage du disque dur doit être accompagnée d'une politique de mot de passe forte. Exemple type d'applications de cryptage, les outils PGP Mobile ou PGP Disk.

L'autre solution consisterait à ne pas avoir d'informations confidentielles sur ces disques mais cela en limite fortement l'usage. Dès lors, les solutions de connexion privée distante s'imposent. "Le VPN SSL revient à la mode. Son principe est simple : le client se connecte à un bureau virtuel et tous les fichiers qu'il aura créés seront effacés à la fin de sa session. Cet accès peut se révéler intéressant mais exige des ressources machines et ne fonctionne qu'avec un réseau à proximité, ce qui réduit de fait la mobilité. D'autres solutions comme Terminal Server ou Citrix, donnent directement accès aux ressources serveurs contrairement au VPN SSL qui se destine à une application", affirme Axelis Ravel D'estinne, consultant sécurité chez Lexsi.

## 2) Appliquer le même niveau de sécurité que pour un poste traditionnel

Antivirus, pare-feu et correctifs de sécurité apportent un premier niveau de sécurité au poste mobile contre les codes malveillants. Encore peu dangereux, les virus mobiles se sont toutefois multipliés ces douze derniers mois. "Depuis Cabir, premier virus théorique à se propager en Bluetooth sur les systèmes Symbian OS, on compte une quarantaine de virus de ce type. Toutefois, pour être contaminé à l'heure actuelle, il faut être équipé d'un système Symbian vulnérable, du Bluetooth et accepter de télécharger une pièce jointe", note Eugenio Correnti, ingénieur sécurité chez F-Secure.

## 3) Vérifier la politique de sécurité des terminaux entrants

Dès lors que l'employé s'absente de l'entreprise pour une longue durée, le risque s'accroît d'une contamination du poste par des virus, vers ou chevaux de troie. Les outils traditionnels de sécurité utilisent une base de signatures qui doit être régulièrement mise à jour. Trois solutions s'offrent alors à l'entreprise : interdire la connexion à distance en désactivant l'accès Internet de la machine, une solution souhaitable si le portable transporte des informations hautement confidentielles ; recourir à un outil de virtualisation du poste client afin de séparer l'usage personnel de l'usage professionnel ; ou créer une zone tampon (DMZ) contrôlant la sécurité du poste à chaque connexion au réseau de l'entreprise. Cette dernière solution n'élimine pas la contamination de la machine mais nettoie l'infection avant de connecter la machine au reste de l'informatique.

## 4) Désactiver les fonctions dangereuses

Les clefs USB constituent un relais potentiel de propagation pour les virus. Les moteurs des antivirus analysent tout lecteur physique, clefs USB comprises mais un risque existe entre le délai d'apparition du virus et la disponibilité de sa signature. Sur un poste de travail fixe, le délai se compte en heures, mais il s'étend en jours sur les mobiles. L'administrateur peut, s'il le juge nécessaire, désactiver l'accès à tout périphérique externe.

Le problème peut être résolu de la même manière pour les réseaux WiFi.

"Concrètement aujourd'hui, si un réseau WiFi est bien installé, il sera sécurisé. Le problème vient de l'ancienneté de certains postes, achetés il y a deux ans, et qui fonctionnent encore avec le protocole Wep. De toute manière, il est recommandé de faire passer ses connexions WiFi par des réseaux privés virtuels. Ainsi, si demain les protocoles WiFi ont été cassés, le VPN continuera de protéger les communications", analyse Laurent Dupuy, consultant sécurité chez Free Security.

## 5) Contrôler le fonctionnement des applications

Des protections disponibles sur les principaux systèmes d'exploitations mobiles comme Windows CE permettent de limiter l'accès aux API systèmes tant que l'application n'a pas été préalablement signée. Cette mesure évite l'utilisation de logiciels potentiellement dangereux (peer-to-peer, messagerie instantanée) et bride les troyens. Le responsable sécurité peut même interdire l'installation de nouveaux composants sur le portable en dehors du réseau de l'entreprise, cela entrave toutefois la liberté offerte par le terminal mobile.

### RUBRIQUES

Nominations  
A lire ailleurs  
Revue des failles  
Ils ont choisi  
Versions  
Agenda

Livres Blancs

### MANAGEMENT

Gestion RH  
Création entreprise  
Emploi cadre  
Fiches pratiques

### ANNUAIRES

Sociétés  
Prestataires  
Logiciels pro  
Carnet  
Encyclopédie  
Formations  
Hotspots Wi-Fi  
Haut débit  
Fonds

Agences médias  
Lobbies



- Copains d'avant
- Cartes de vœux
- Journal des Femmes
- Actualités
- Fonds d'écran
- Galerie photos
- Vos livres
- Internet Pratique
- Photo numérique
- Recettes de cuisine

Tous les dossiers

### VOTRE HIGH-TECH

Eligibilité  
Test connexion  
Guides d'achat  
Comparateur Prix  
Télécharger  
Livres

### CONTACTS

Newsletters  
Contacts  
Publicité



- Benchmark.fr
- Séminaires
- Etudes Publicité et marketing sur

## 6) Sensibiliser les utilisateurs aux risques

Tout comme le poste de travail, le terminal mobile implique des risques et donc des procédures de sécurité quotidiennes dont il faut avertir l'utilisateur. Les cabinets de conseil en sécurité recommandent de porter l'effort de communication notamment sur la sécurisation des données confidentielles et la nécessité d'une utilisation raisonnée de la connexion à distance. Pour éviter une dégradation des conditions de sécurité, il convient de réaliser un diagnostic régulier de la machine. A cette occasion, le responsable sécurité pourra rappeler les principaux risques à l'utilisateur de l'appareil mobile.

## 7) Séparer les connexions des terminaux mobiles du reste du réseau

La séparation s'effectue soit en installant un réseau virtuel (VLAN), soit en limitant les droits d'accès aux applications réseaux ou en ne donnant accès qu'à une base secondaire répliquée à partir de la base principale. La séparation possède un double intérêt : elle évite la propagation d'un virus au reste de l'infrastructure en cas d'infection et elle restreint toute tentative d'accès distant non autorisé même en cas d'authentification réussie.

## 8) Harmoniser la gestion de son parc mobile

La diversité des protocoles et des fonctionnalités des terminaux mobiles complique l'administration de la sécurité. En revanche, la diversité garantit une meilleure étanchéité du réseau face aux différentes menaces mobiles actuelles qui s'appuient comme le virus CommWarrior sur la connexion Bluetooth disponibles sur une catégorie d'appareils bien déterminés. "Les constructeurs ont fait beaucoup de progrès pour protéger tout ce qui tourne autour de la communication Bluetooth et de la pile Bluetooth. Avant, avec un certain type d'émetteur, une attaque à des distances proches du kilomètre était possible", explique Laurent Dupuy.

## 9) Contrôler les connexions Internet par le biais de smartphones

Une menace possible des smartphones se situe dans la création de passerelles Internet. Equipés d'une connexion Bluetooth et GPRS, ces appareils peuvent servir de passerelles Internet à des postes d'entreprises qui passent ainsi outre les protections habituelles de proxy, pare-feu et filtrages d'URL. Utiliser un téléphone mobile comme modem USB ou Bluetooth nécessite toutefois des modifications systèmes. L'administrateur sécurité pourra détecter les modems non autorisés via des outils d'analyse de flux puis vérifier l'état du système sur ces terminaux.

## 10) Réaliser des sauvegardes régulières de l'image du système

Eloignés de l'entreprise, les documents présents sur les terminaux mobiles ne peuvent être toujours sauvegardés au même rythme que les postes de travail. Pourtant, les PDA ou les smartphones contiennent désormais des données sensibles (photos, vidéos, carnet d'adresse, mails ou fichiers textes). Il convient donc d'assurer régulièrement cette sauvegarde, par exemple à l'occasion d'une connexion réseau en comparant la date de la dernière sauvegarde des données avec la date actuelle.

 [En savoir plus](#)

[10 conseils pour mettre en place un réseau local sans fil](#)

 [Dossier](#) [Mobilité](#)



[Qui sommes-nous ?](#) | [Société](#) | [Contacts](#) | [Publicité](#) | [PA Emploi](#) | [Presse](#) | [Recrutement](#) | [Tous nos sites](#) | [Données personnelles](#)

© Benchmark Group, 4 rue Diderot. 92156 Suresnes Cedex