Salon sécurité : Terminaux mobiles, clés USB sont des maillons faibles

Les terminaux mobiles sont désormais une réalité en termes de parcs dans beaucoup d'entreprises. Réseaux haut débit et capacité de stockage à la hausse permettent aux cadres et toutes les équipes nomades de rester en contact et d'échanger des informations avec leur entreprise. En jeu: des gains de temps et, donc, de productivité.

Mais le succès de la mobilité professionnelle a son revers: la sécurité. Pointsec, groupe suédois créé en 1988 est classé comme le leader sur le marché de la protection des données mobiles. Un secteur en plein essor. Le groupe a déployé pas moins de 5 millions de licences, et compte parmi ses clients, le FBI.

« *Aujourd'hui, les ventes de PC de salon sont en chute libre* », indique Mikaël Taillepied, Directeur Général de Pointsec, « *le portable est à la mode et le réseau sans fil émerge. L'on assiste également à la prolifération du push mail sur les smartphones et les PDA, il y a une demande forte d'accès à l'information, seulement il y a un risque réel puisque 50% des intrusions sont faites à partir de données volées et perdues.* »

Selon le dernier rapport du Clusif (Club de la Sécurité de l'Information Français), 37% des PME ont constaté au moins un vol en 2005, contre 6% en 2003. Ce taux passe à 65% (!) chez les entreprises de plus de 1.000 salariés. En moyenne, 44% des entreprises interrogées par le Clusif ont constaté des vols ou des disparitions de matériel en 2005. Or, selon une autre étude menée sur le salon Infosecurity en 2005, 81% des PDA stockent des contacts professionnels, 59% des agendas professionnels et 27% des données d'entreprises.

De la même façon, une étude menée en 2005 par Pointsec sur les pertes d'appareils mobiles dans les lieux publics dans la ville de Copenhague montre que 566 PDA ont été perdus en 6 mois dans les taxis, soit une augmentation de 350% depuis 2001. 11.971 téléphones portables ont également été oubliés dans l es taxis. Dans les six derniers mois, 5.838 Pocket PC et 4.973 laptops ont été perdus dans les taxis londoniens. Des chiffres colossaux… Sachant que 60% des vols de données proviennent d'un appareil volé ou perdu contre seulement 25% pour une intrusion de réseau, il devient alors critique pour une entreprise de protéger ces terminaux en allant plus loin que les outils fournis par les fabricants comme l'éternel duo 'login-password'.

Si la protection des données est souvent négligée par les utilisateurs du réseau, désormais le mouvement s'accélère notamment grâce à une législation et des obligations de plus en plus fortes.

Pour Taillepied, « *l'aspect mobile a été pris en compte tardivement, mais depuis peu l'on assiste à une véritable prise de conscience* ».

D'après lui,« *la sécurité des données mobiles passe aussi bien par l'aspect purement réseau que physique.* » C'est d'ailleurs là le c?ur de métier de Pointsec qui se propose de protéger le terminal dès son ouverture en pré-boot, une protection plus forte qu'un post-boot, un pirate suffisamment érudit pouvant facilement contourner le boot d'un ordinateur grâce à une clé USB et un freeware bien connu et largement disponible sur la Toile.

Du coté de la politique de sécurité, Pointsec conseille de classifier les données par ordre d'importance, de déterminer un niveau de sécurité selon évaluation et une fois cela terminé de rapporter le résultat de cet audit à l'activité de l'entreprise. Pour définir les applications mobiles à surveiller, il est impératif d'impliquer les utilisateurs qui sont souvent mal informés des risques qu'ils prennent pour l'activité de leur société.

Mikaël Taillepied insiste sur cet aspect qui est *« un point important à ne surtout pas mettre en second plan. »*

Du point de vue de l'utilisateur, l'authentification doit être simple et le fonctionnement de la protection relativement transparent. Car dès qu'il y a interaction avec l'humain, le risque est plus grand.

Pour la sécurité physique du réseau, Taillepied insiste sur *« une authentification forte »* comme avec des tokens ou des cartes à puces, qui ne sont pas encore suffisamment déployés. Enfin, et c'est là ou Pointsec intervient, la meilleure protection reste le chiffrement de tous les secteurs du disque dur. Installées en couche basse, les solutions de Pointsec pour Notebook ou PDA ne posent pas de problèmes d'interopérabilité.

Actuellement, Pointsec permet de sécuriser pas moins de 30 cartes SD et offre un outil de développement de drivers avec son logiciel, ce qui limite les risques. Notons qu'une version bêta de Pointsec existe pour la RC1 et la RC2 de Vista.

L'algorithme de chiffrement recommandé par Pointsec est l'AES 128 et 256 bits. En charge supplémentaire, le chiffrement du disque dur entraîne une perte de 1,5% de capacité d'utilisation. Il faut compter en moyenne une heure pour chiffrer 10GB.

Pour autant, la question du déploiement de ce type de solution se pose. Surtout dans le cadre d'immenses flottes. *« Nous développons des kits d'installation centralisés multi-OS. Ensuite, il suffit de 'pousser' l'outil de protection vers les terminaux, à la manière du push e-mail. Ce qui se fait en toute transparence «* .

Preuve que cette prise de conscience existe bien, le chiffrement des PDA représente désormais 40% du chiffre d'affaires de Pointsec contre 20% il y a un an.

Le cas des clés USB

Elles sont partout et traînent dans les poches de dizaines de milliers de salariés. Il faut dire qu'elles sont quasiment données aujourd'hui. Mais ces supports de stockage amovibles constituent également un danger pour le SI de l'entreprise. Elles peuvent être à l'origine de l'injection de codes malveillants dans un poste de travail. A l'inverse, elles permettent d'aspirer des données sensibles. *« Elles échappent complètement au contrôle des entreprises »*, souligne Mikaël Taillepied.

Ainsi, en une année, le nombre de personnes ayant reconnu avoir eu recours à l'utilisation de clés USB pour enregistrer les données de leur entreprise sur leur lieu de travail a quasiment doublé. Cependant, les équipes informatiques sont persuadées que la majorité d'entre elles ne sont pas sécurisées. Un échantillon de 2/3 des professionnels informatiques qui utilisent eux mêmes ces médias amovibles au travail admettent qu'ils ne les protègent pas par un chiffrement même s'ils

sont conscients des dangers associés.

Dans le même temps, 56% des employés enregistrent les informations de l'entreprise sur leurs clés USB. Par ailleurs, 65% des professionnels informatiques admettent que les médias amovibles représentent potentiellement une bombe à retardement. Seulement 21% des médias amovibles de l'entreprise sont sécurisés par des mots de passe ou un chiffrement. Certaines entreprises (12%) en interdisent l'usage en neutralisant par exemple les ports USB des machines. Ce qui n'est pas tenable. Une autre solution consiste alors à chiffrer les données qui sortent d'un PC comme le préconise Pointsec.

« L'utilisateur peut transférer un fichier vers un support amovible, mais sa lecture a posteriori sera bloquée si telle est la volonté de l'entreprise « , poursuit le dg. *« Notre recommandation est d'introduire des procédures strictes sur l'usage des médias amovibles dans les lieux de travail et d'investir dans un logiciel de chiffrement qui permettra aux administrateurs de forcer le chiffrement de toutes les données enregistrées dans un média amovible. Les entreprises réaliseront bientôt que ce type de logiciel est tout aussi vital et non coûteux que l'usage d'un logiciel anti-virus. »*, explique de son côté Martin Allen, Directeur de Pointsec UK.

Toute l'information du Salon Securité/Stockage sur l e blog de Silicon/VNU