

La mobilité des données retaille les contours de la confidentialité

Les ordinateurs portables ou les clés USB constituent plus que jamais l'une des premières causes de fuites d'informations.

JACQUES MEDINA*

La mobilité des utilisateurs et la prolifération des supports de données mobiles fragilisent les méthodes de défense traditionnelles des entreprises. Selon Gartner, 47% des données des sociétés résident sur des supports mobiles. Un chiffre qui va croissant. Mais la mobilité même de ces supports – allant de l'ordinateur portable à la clé USB – les prédispose à pouvoir être perdus, volés ou contaminés. Le défi est donc de tirer parti de leurs avantages tout en limitant les risques qui en découlent.

De nombreuses entreprises ressentent de manière pressante le besoin de résoudre la question. Selon l'importance des données en circulation, elles choisiront ou non de prendre des mesures de protection. Quelles sont les protections recherchées? En cas de vol ou de perte d'un ordinateur portable ou d'une clé USB, les entreprises veulent la garantie que les données ne puissent pas être exploitées. Elles veulent aussi être certaines qu'une clé USB ne puisse pas introduire de programmes malveillants dans l'entreprise. Enfin, elles veu-

lent pouvoir éviter que des données sensibles de l'entreprise soient transférables sur le support de données d'une personne extérieure à l'entreprise.

Le cryptage constitue la clé de la confidentialité

Toutes ces protections existent. Il est aujourd'hui possible de crypter le contenu des disques durs et des supports mobiles, d'assurer la gestion des ports USB, de filtrer et de vérifier le contenu des supports USB. Il est même possible d'assurer la traçabilité des données que ces supports contiennent. Quelques détails.

Protection des ordinateurs fixes et portables: le cryptage. Crypter le disque dur d'un ordinateur portable ou de bureau offre deux paliers de sécurité: tout d'abord, les données ne peuvent pas être lues par des tiers en cas de vol ou de perte; ensuite, une seule personne (l'utilisateur autorisé) peut se connecter à la machine, car il n'est pas possible d'en contourner la protection. Le principe: un petit système d'exploitation est exécuté avant Windows. Son accès par login/mot de passe est synchronisé avec celui de Windows, ce qui signifie que l'utilisateur in-

trouduit simplement son mot de passe un peu plus tôt qu'il ne le ferait normalement pour accéder à son bureau Windows. Ainsi, il est impossible à une tierce personne d'accéder à la machine à moins de reformater complètement le disque dur, ce qui met de facto les données à l'abri. La gestion du cryptage des ordinateurs fixes et portables peut être effectuée de manière centralisée.

Supports USB: cryptage, protection et contrôle. Il est possible de crypter les données enregistrées sur un support de données USB afin d'en assurer la confidentialité. Mais il peut être approprié d'aller plus loin, puisque les supports de données mobiles peuvent s'avérer des vecteurs de contamination s'ils ramènent dans l'entreprise des fichiers exécutables pouvant vulnérabiliser le réseau. Pour éliminer ce risque, on peut détecter et contrôler l'utilisation de chaque support de données dans l'environnement informatique de l'entreprise. Cela permet d'assurer un contrôle précis des types de périphériques et de fichiers autorisés. Concrètement, chaque fois qu'un support de données est inséré dans le port USB d'un ordinateur de

l'entreprise, un contrôle de contenu avec recherche de virus est effectué afin d'assurer l'intégrité du réseau. Une telle solution fournit aussi un historique de tous les fichiers qui ont transité sur chaque support. Ce suivi se fait par l'intermédiaire d'un échange d'informations entre la station de travail, où l'utilisateur connecte son support de données, et le serveur. Le suivi a lieu en temps réel si l'utilisateur du support de données se trouve dans l'entreprise. S'il est à l'extérieur, l'échange a lieu dès qu'il se connecte au réseau ou au plus tard à son retour au bureau

Il faut authentifier tous les supports de données

Le propriétaire d'un support de données protégé peut accéder aux données qu'il contient depuis n'importe quel ordinateur moyennant un login/mot de passe authentifié. En sens inverse, il faut toutefois relever que le contrôle des ports USB peut compliquer l'interaction avec le monde extérieur. Les personnes extérieures à l'entreprise ne peuvent pas y utiliser leurs propres supports de données, puisque seuls ceux qui sont authentifiés y sont acceptés. Ce

problème peut être résolu en mettant à disposition un PC «kiosque» non connecté au réseau, à travers lequel il est possible d'échanger des données sans faire appel à l'IT.

De tels outils sont faciles à mettre en place. Le plus long travail n'est d'ailleurs pas leur installation, mais la préparation préalable: définir ce qu'il faut autoriser, à qui, et gérer les exceptions. Une fois ce travail de fond effectué, la mise en œuvre d'une solution efficace ne présente pas de difficulté particulière.

Enfin, il n'est peut être pas inutile de préciser que les CD-ROM et les appareils de photos numériques ou les iPods représentent le même danger que les supports USB, et qu'ils peuvent être protégés de la même manière.

Les supports de données mobiles sont l'une des premières causes de fuites de données confidentielles. Les sécuriser peut s'avérer intéressant pour toute entreprise qui souhaite se mettre à l'abri de tels risques sans pour autant compliquer la vie des utilisateurs ni ralentir leurs procédures de travail.

*Security Architect, Navixia