

**S curit  : IT, L'homme est toujours le maillon faible de la cha ne**  
**S curit **

Post  par : JerryG

Publi e le : 10/12/2012 15:00:00

Le nombre de menaces int rieures au sein des entreprises - identifi  par le CLUSIF dans son rapport 2012 - est assez  difiant. Parmi les entreprises interrog es, 25% ont subi un incident de s curit  de l'information cons cutif   **une  « attaque  » d'origine interne**, au cours des 12 derniers mois.

Il peut s'agir d'infections involontaires par virus, d'erreurs d'utilisation, de vol de mat riel portable, de n gligence ou encore de malveillance. Ainsi il n'est pas rare que des salari s licenci s emportent massivement des informations confidentielles ; en ces temps de crise, ce type de comportement est de plus en plus fr quent.



  Si les cas de dommages volontaires sont marginaux et difficilement  vitables, les risques li s   une pratique insouciance des technologies mises   la disposition des employ s peuvent, eux,  tre circonscrits.

**Parmi les recommandations citons :**

- la gestion des identit s
- le chiffrement
- la biom trie
- la mise en  uvre d'architectures VLAN qui isolent judicieusement les segments entre eux,
- l'utilisation de solutions de stockage centralis  des donn es

**L'homme est toujours le maillon faible de la cha ne**, rappelle Emmanuel Lehmann, consultant sp cialis  et auteur du  « Petit trait  d'attaques subversives contre les entreprises  » (Chiron, 2009).

Il est donc important d'appliquer une consigne simple, favoris e par la mise en  uvre d'une solution de s curit  centralis e : aucun fichier n'est stock  localement sur ordinateur. Les collaborateurs acc dent   leur environnement et   leurs informations, via une connexion s curis e, y compris en situation de mobilit . Ainsi si le terminal est vol  ou perdu, personne ne peut acc der aux donn es confidentielles. Dans ce genre de configuration, il est  galement plus simple de prot ger les fichiers stock s contre les virus.

Nous sommes bien loin des traditionnels Antivirus/Firewall ! Pour limiter l'impact des menaces internes, il est par exemple possible de combiner des solutions de segmentation logique du LAN (adresses MAC, authentification, numéro de port, protocoles...) et l'encapsulation des informations, avec des systèmes de gestion des identités et des droits d'accès, qui tiennent compte des profils et des rôles des collaborateurs.

« *Interdire ou autoriser n'est souvent pas un réglage suffisamment fin pour les entreprises* », remarque **Thierry Karsenti**, titulaire de la Chaire de recherche du Canada, sur les TIC. Il est évident qu'avec le développement de la mobilité des collaborateurs, il devient essentiel de mettre en œuvre des systèmes de chiffrement, de contrôle d'accès avancé, via des solutions d'authentification forte, voire la biométrie. Ainsi par exemple, la reconnaissance des empreintes digitales par ordinateur portable réduit considérablement les risques de vol d'informations.

« **Les autorités publiques prennent parfois des mesures exemplaires** afin que les entreprises protègent plus efficacement leurs données sensibles et augmentent leur intelligence économique. Ainsi, en Grande Bretagne, en août dernier, la Financial Services Authority infligeait une amende record de 2,7 millions d'euros à une grande compagnie d'assurance pour la perte de données personnelles de quelque 46000 clients, incluant numéros de comptes et de cartes bancaires.

Malgré les prises de conscience, les recommandations d'usage, les restrictions, et la mise en place de solutions qui limitent les risques, une faille peut toujours exister... Dès lors l'utilité de mener un audit des modes de fonctionnement interne de l'entreprise, sans paranoïa, pour pointer les faiblesses éventuelles, évaluer les impacts, et trouver le bon dosage entre pilotage technique et management adéquat du comportement des salariés.