SÃ©curitÃ© : IT, Lâ□□homme est toujours le maillon faible de la chaÃ®ne
SÃ©curitÃ©
PostÃ© par : JerryG
PubliÃ©e le : 10/12/2012 15:00:00

Le nombre de menaces intÃ©rieures au sein des entreprises - identifiÃ© par le CLUSIF dans son rapport 2012 - est assez Ã©difiant. Parmi les entreprises interrogÃ©es, 25% ont subi un incident de sÃ©curitÃ© de lâ□□information consÃ©cutif Ã **une Â« attaque Â» dâ□□origine interne**, au cours des 12 derniers mois.

Il peut sâ□□agir dâ□□infections involontaires par virus, dâ□□erreurs dâ□□utilisation, de vol de matÃ©riel portable, de nÃ©gligence ou encore de malveillance. Ainsi il nâ□□est pas rare que des salariÃ©s licenciÃ©s emportent massivement des informations confidentielles ; en ces temps de crise, ce type de comportement est de plus en plus frÃ©quent.

â□¨Si les cas de dommages volontaires sont marginaux et difficilement Ã©vitables, les risques liÃ©s Ã une pratique insouciante des technologies mises Ã la disposition des employÃ©s peuvent, eux, Ãªtre circonscrits.

Parmi les recommandations citons :

- la gestion des identitÃ©s

- le chiffrement

- la biomÃ©trie

- la mise en Å□uvre dâ□□architectures VLAN qui isolent judicieusement les segments entre eux,

- lâ□□utilisation de solutions de stockage centralisÃ© des donnÃ©es

Lâ□□homme est toujours le maillon faible de la chaÃ®neâ□□ , rappelle Emmanuel Lehmann, consultant spÃ©cialisÃ© et auteur du Â« Petit traitÃ© dâ□□attaques subversives contre les entreprises Â» (Chiron, 2009).

Il est donc important dâ□□appliquer une consigne simple, favorisÃ©e par la mise en Å□uvre dâ□□une solution de sÃ©curitÃ© centralisÃ©e : aucun fichier nâ□□est stockÃ© localement sur ordinateur. Les collaborateurs accÃ¨dent Ã leur environnement et Ã leurs informations, via une connexion sÃ©curisÃ©e, y compris en situation de mobilitÃ©. Ainsi si le terminal est volÃ© ou perdu, personne ne peut accÃ©der aux donnÃ©es confidentielles. Dans ce genre de configuration, il est Ã©galement plus simple de protÃ©ger les fichiers stockÃ©s contre les virus.

Nous sommes bien loin des traditionnels Antivirus/Firewall ! Pour limiter lâ□□impact des menaces internes, il est par exemple possible de combiner des solutions de segmentation logique du LAN (adresses MAC, authentification, numÃ©ro de port, protocoles...) et dâ□□encapsulation des informations, avec des systÃ¨mes de gestion des identitÃ©s et des droits dâ□□accÃ¨s, qui tiennent compte des profils et des rÃ´les des collaborateurs.

Â« *Interdire ou autoriser nâ□□est souvent pas un rÃ©glage suffisamment fin pour les entreprises* Â», remarque **Thierry Karsenti,** titulaire de la Chaire de recherche du Canada, sur les TIC. Il est Ã©vident quâ□□avec le dÃ©veloppement de la mobilitÃ© des collaborateurs, il devient essentiel de mettre en Å□uvre des systÃ¨mes de chiffrement, de contrÃ´le dâ□□accÃ¨s avancÃ©, via des solutions dâ□□authentification forte, voire la biomÃ©trie. Ainsi par exemple, la reconnaissance des empreintes digitales par ordinateur portable rÃ©duit considÃ©rablement les risques de vol dâ□□informations.

â□¨**Les autoritÃ©s publiques prennent parfois des mesures exemplaires** afin que les entreprises protÃ¨gent plus efficacement leurs donnÃ©es sensibles et augmentent leur intelligence Ã©conomique. Ainsi, en Grande Bretagne, en aoÃ»t dernier, la Financial Services Authority infligeait une amende record de 2,7 millions dâ□□euros Ã une grande compagnie dâ□□assurance pour la perte de donnÃ©es personnelles de quelque 46000â□□clients, incluant numÃ©ros de comptes et de cartes bancaires.

MalgrÃ© les prises de conscience, les recommandations dâ□□usage, les restrictions, et la mise en place de solutions qui limitent les risques, une faille peut toujours exister... Dâ□□ou lâ□□utilitÃ© de mener un audit des modes de fonctionnement interne de lâ□□entreprise, sans paranoÃ¯a, pour pointer les faiblesses Ã©ventuelles, Ã©valuer les impacts, et trouver le bon dosage entre pilotage technique et management adÃ©quat du comportement des salariÃ©s.