SÃ©curitÃ© informatique : Le danger vient aussi de l' intÃ©rieur

SÃ©curitÃ©
PostÃ© par : JPilo
PubliÃ©e le : 7/10/2014 11:30:00

Alors que lâ□□attention gÃ©nÃ©rale est tournÃ©e vers la protection des rÃ©seaux et des fichiers numÃ©riques sensibles des grandes entreprises et des gouvernements contre les attaques externes, les menaces les plus communes et les plus dangereuses proviennent de lâ□□intÃ©rieur des entreprises.

Le numÃ©ro de septembre de Harvard Business Review souligne Â« *Le danger intÃ©rieur* Â» et confirme une prise de conscience justifiant lâ□□adoption de solutions telles que celles proposÃ©es par Varonis Systems, Inc., le principal fournisseur de solutions logicielles pour les donnÃ©es dâ□□entreprise non structurÃ©es dâ□□origine humaine.

Â« *Le personnel interne dâ□□une entreprise peut causer beaucoup plus de torts que des pirates de lâ□□extÃ©rieur, car ils ont beaucoup plus de possibilitÃ©s et les accÃ¨s nÃ©cessaires aux systÃ¨mes pour cela* Â», indiquent David Upton et Sadie Creese, professeurs Ã lâ□□universitÃ© dâ□□Oxford et codirecteurs du programme de recherche Corporate Insider Threat Detection (dÃ©tection des menaces internes dans les grandes entreprises), un projet international destinÃ© Ã aider les sociÃ©tÃ©s Ã dÃ©couvrir et neutraliser de telles menaces.

Le texte de Harvard Business Review prÃ©cise Ã©galement : Â« *Selon diverses estimations, plus de 80 millions dâ□□attaques internes se produisent aux Ã□tats-Unis chaque annÃ©e. Mais ce nombre pourrait Ãªtre bien plus Ã©levÃ©, car elles restent souvent non signalÃ©es. Les dÃ©gÃ¢ts se comptent en dizaines de milliards de dollars par an. De nombreuses entreprises reconnaissent quâ□□elles ne disposent pas encore des dispositifs de protection adÃ©quats leur permettant de dÃ©tecter ou de prÃ©venir les attaques provenant de lâ□□intÃ©rieur. Une des raisons Ã cela est quâ□□elles refusent encore de reconnaÃ®tre lâ□□ampleur de la menace.* Â»

Dans une enquÃªte menÃ©e en 2013 auprÃ¨s de plus de 120 entreprises, Varonis soulignait que la plupart des fuites de propriÃ©tÃ© intellectuelle provoquÃ©es par des accÃ¨s internes nâ□□Ã©taient pas malveillantes ou mÃªme intentionnelles. Parmi les causes, nous identifiions les collaborateurs qui tÃ©lÃ©chargent des donnÃ©es sensibles relatives Ã leur travail vers des comptes cloud personnels, la mauvaise connaissance des accords de confidentialitÃ©, le manque de formation et de communication rÃ©guliÃ¨re sur la protection des donnÃ©es sensibles ainsi que lâ□□absence dâ□□outils permettant aux entreprises de gÃ©rer et de contrÃ´ler les accÃ¨s aux fichiers privÃ©s. Les rÃ©sultats de lâ□□enquÃªte indiquent que seulement 46 % des rÃ©pondants ont Ã©tÃ© invitÃ©s Ã restituer leurs contenus numÃ©riques en quittant leurs fonctions.

Entre autres conseils, les chercheurs recommandent de superviser lâ□□accÃ¨s et lâ□□utilisation des donnÃ©es par les collaborateurs. En dÃ©crivant lâ□□Ã©tude, le professeur Upton rappelle :

Â« *Nous installons des alarmes antivol pour empÃªcher les gens de pÃ©nÃ©trer dans nos maisons. Mais ce sont ceux que nous laissons entrer qui constituent le problÃ¨me. Il en est de mÃªme pour les entreprises. Les principes utilisÃ©s pour se dÃ©fendre contre les menaces externes ne fonctionnent tout simplement pas contre les personnes dÃ©jÃ dans la place. Au cours de ces derniÃ¨res annÃ©es, les entreprises ont laissÃ© de nombreuses personnes entrer dans leur maison.*

Cela peut se faire par le recours aux services de Cloud Computing, du fait dâ□□employÃ©s *apportant leurs propres pÃ©riphÃ©riques au travail ou en raison de la prolifÃ©ration des mÃ©dias sociaux et de lâ□□utilisation des Big data. Bien que toutes ces personnes disposent dâ□□un accÃ¨s lÃ©gitime aux actifs numÃ©riques de lâ□□entreprise, la possibilitÃ© dâ□□en faire un usage malveillant, intentionnel ou non, est augmentÃ©e dans des proportions Ã©normes* Â».

[***Pour de plus amples informations sur cette Ã©tude.***]

 Comme le rappelle David Gibson, vice-prÃ©sident de Varonis

Â« *le travail effectuÃ© Ã   Oxford par les professeurs Upton et Creese est dâ□□une grande importance, car les menaces internes sont encore sous-estimÃ©es et souvent incomprises. La croissance explosive des donnÃ©es non structurÃ©es, courriers Ã©lectroniques, feuilles de calcul, prÃ©sentations, documents et autres fichiers crÃ©Ã©s par les employÃ©s, a amplifiÃ© les problÃ¨mes inhÃ©rents Ã   lâ□□absence de contrÃ´le des accÃ¨s internes.*

La technologie de mÃ©tadonnÃ©es brevetÃ©e de Varonis nous permet dâ□□aider les entreprises Ã   prendre le contrÃ´le de lâ□□essentiel, Ã   savoir qui possÃ¨de quels fichiers, qui a potentiellement accÃ¨s et qui accÃ¨de rÃ©ellement aux donnÃ©es, qui doit et qui ne doit pas y avoir accÃ¨s, qui abuse de ses possibilitÃ©s dâ□□accÃ¨s, et quels sont les fichiers sensibles exposÃ©s. Â»