Quatre conseils pour rester au top sur les questions de sÃ©curitÃ©
SÃ©curitÃ©
PostÃ© par : JPilo
PubliÃ©e le : 21/3/2013 13:30:00

Ces derniÃ¨res annÃ©es, les histoires de **fuites de donnÃ©es retentissantes et trÃ¨s mÃ©diatisÃ©es** nâ□□ont pas manquÃ©. Par exemple, tout le monde a entendu parler de lâ□□affaire des documents secrets du gouvernement britannique retrouvÃ©s dans un train en juin 2008.

On se souvient que ces documents expliquaient en dÃ©tail la politique de lutte du Royaume-Uni contre le financement du terrorisme, le trafic de drogue et le blanchiment dâ□□argentâ□¦

Si elles sont trÃ¨s mÃ©diatisÃ©es, les affaires de ce type sont cependant raresâ□¦ On parle beaucoup moins des milliers dâ□□entreprises qui se font pincer pour avoir manipulÃ© ou utilisÃ© Ã mauvais escient des informations confidentielles sur leurs clients. Dans une Ã©tude rÃ©cente sur la sÃ©curitÃ© des donnÃ©es, prÃ¨s de la moitiÃ© des 500 responsables informatiques interrogÃ©s ont reconnu avoir dÃ©jÃ Ã©tÃ© confrontÃ©s Ã une violation de donnÃ©es.**Bruno Labidoire**, Directeur Technique Europe du Sud dÃ©taille la question.

Ce genre dâ□□Ã©vÃ©nement est terriblement dommageable en termes dâ□□image mais, de plus, les entreprises convaincues de violation de donnÃ©es sâ□□exposent Ã des sanctions de plus en plus sÃ©vÃ¨res. Par exemple, au Royaume-Uni, lâ□□Information Commissionerâ□□s Office (ICO), un organisme public indÃ©pendant a Ã©tÃ© crÃ©Ã© pour promouvoir lâ□□accÃ¨s aux informations officielles et protÃ©ger les donnÃ©es personnelles. Celui-ci a durci son approche et a collectÃ© 2 millions de livres sterling suite aux amendes distribuÃ©es aux entreprises qui enfreignaient ses consignes.

Dans notre Ã©conomie de lâ□□information, les donnÃ©es dâ□□une organisation sont son principal actif. Mais si des donnÃ©es privÃ©es sont rendues publiques ou tombent entre de mauvaises mains, cet actif peut aussi causer sa chute. Le dÃ©veloppement commercial, lâ□□implantation de nouveaux territoires, les fusions-acquisitions sont autant dâ□□activitÃ©s qui rendent la question de la protection des donnÃ©es de plus en plus complexe. Quâ□□est-ce quâ□□un professionnel de la sÃ©curitÃ© doit faire pour sâ□□assurer que les efforts de son entreprise vont dans le bons sens et la mettent Ã lâ□□abri du danger ?

1. ConnaÃ®tre les lois et les rÃ©glementations

Selon une Ã©tude rÃ©cente, 65% des responsables informatiques estiment quâ□□il est difficile de respecter les rÃ©glementations sur la confidentialitÃ© et la protection des donnÃ©es. Le fait quâ□□en Europe les lois sur la confidentialitÃ© des donnÃ©es diffÃ¨rent dâ□□un pays Ã lâ□□autre suffit Ã expliquer pourquoi. Les professionnels de la sÃ©curitÃ© informatique doivent faire en sorte dâ□□Ãªtre au courant de tous les textes de loi et rÃ©glementations qui sortent pour rÃ©agir en consÃ©quence et rÃ©duire le risque de violation de donnÃ©es.

2. Rester informÃ© sur ce qui se passe et les nouveaux risques

Les professionnels de la sÃ©curitÃ© doivent aussi faire leur travail personnel. Il est indispensable quâ□□ils se tiennent au courant de ce qui se passe, des problÃ©matiques qui apparaissent, quâ□□ils sachent qui a Ã©tÃ© victime dâ□□une fuite de donnÃ©es et comment cela sâ□□est produit. Actuellement par exemple, lâ□□origine la plus frÃ©quente des fuites de donnÃ©es est la perte dâ□□un ordinateur portable ou dâ□□un appareil mobile contenant des donnÃ©es de lâ□□entreprise. Les responsables sÃ©curitÃ© sont-ils conscients de ce problÃ¨me, en prennent-ils toute la mesure et si oui, que font-il pour le rÃ©soudre ?

Ils doivent sâ□□intÃ©resser activement aux problÃ©matiques qui Ã©mergent, lire et se documenter, participer aux confÃ©rences sur ces sujets, Ã©couter ce que leurs homologues ont Ã dire sur la maniÃ¨re dont les criminels, mais aussi des personnes de lâ□□entreprise bien intentionnÃ©es ou au contraire malveillantes, mettent Ã mal ou dÃ©jouent la sÃ©curitÃ©, et sur ce quâ□□il est possible faire pour rÃ©duire les risques.

3. Communiquer, communiquer, communiquer

Les professionnels de la sÃ©curitÃ© ne doivent pas se contenter de communiquer avec leurs homologues. Il est essentiel quâ□□ils Ã©changent avec les membres du comitÃ© exÃ©cutif de lâ□□entreprise pour sâ□□assurer que les mesures prises pour Ã©viter les fuites de donnÃ©es sont les bonnes. Les membres du ComEx qui ne sâ□□occupent gÃ©nÃ©ralement pas de technologie, typiquement le directeur gÃ©nÃ©ral et le directeur financier, doivent Ã©galement Ãªtre dans la boucle si le responsable sÃ©curitÃ© veut dÃ©montrer son utilitÃ© et justifier lâ□□investissement dans les technologies et les services nÃ©cessaires pour protÃ©ger lâ□□entreprise.

4. Veiller Ã protÃ©ger les rÃ©sultats

Les professionnels de la sÃ©curitÃ© doivent toujours avoir Ã lâ□□esprit la performance et les rÃ©sultats de lâ□□entreprise. Lâ□□arbitrage peut Ãªtre difficile entre consacrer des ressources Ã©normes au dÃ©ploiement des technologies et des services de sÃ©curitÃ© et prendre le risque, jamais certain, quâ□□une fuite de donnÃ©es se produise. Câ□□est aux professionnels de la sÃ©curitÃ© quâ□□il incombe de trouver le bon Ã©quilibre.

Quand lâ□□information est le principal actif dâ□□une organisation, celle-ci doit sâ□□assurer quâ□□elle fait tout ce quâ□□il est possible de faire pour protÃ©ger cet actif. Cela lâ□□aidera Ã Ã©viter les piÃ¨ges et les risques de la violation de donnÃ©es. En suivant ces quelques conseils, les responsables sÃ©curitÃ© peuvent facilement rÃ©duire le risque de se voir attaquer sur ce qui relÃ¨ve de leur responsabilitÃ©.

Â