Un risque croissant de vol de donnÃ©es en raison de â□□menaces internesâ□□
Internet
PostÃ© par : JPilo
PubliÃ©e le : 9/4/2014 11:00:00

Cette Ã©tude commanditÃ©e par Vormetric met en Ã©vidence le faible contrÃ´le des utilisateurs privilÃ©giÃ©s au sein des entreprises franÃ§aises et la reconnaissance du chiffrement comme la technologie la plus efficace pour prÃ©venir le risque des menaces intÃ©rieures. En outre, 53% des entreprises europÃ©ennes trouvent ces menaces plus difficiles Ã dÃ©tecter quâ□□auparavant. Vormetric, lâ□□un des principaux experts de la sÃ©curitÃ© des donnÃ©es de lâ□□entreprise pour les environnements physiques, cloud ou virtuels, a rÃ©vÃ©lÃ© aujourdâ□□hui les conclusions de lâ□□enquÃªte europÃ©enne Â« Insider Threat Â» dÃ©diÃ©e aux menaces internes, conduite en 2014 par le cabinet dâ□□analystes Ovum.

Cette enquÃªte, rÃ©alisÃ©e auprÃ¨s de plus de 500 dÃ©cideurs dans le domaine des hautes technologies de moyennes et grandes entreprises au Royaume-Uni, en France, en Allemagne, conclut que seuls 9% des entreprises se sentent Ã lâ□□abri des menaces provenant de lâ□□intÃ©rieur, avec presque la moitiÃ© des sondÃ©s en France (42%) reconnaissant que ce sont les Â« utilisateurs privilÃ©giÃ©s Â» (administrateurs systÃ¨mes, de bases de donnÃ©es, rÃ©seaux, etc.) qui reprÃ©sentent le plus grand risque pour leur entreprise.

Les menaces intÃ©rieures ne proviennent plus seulement des utilisateurs habituels ayant des droits dâ□□accÃ¨s lÃ©gitimes et qui en abuseraient pour voler des donnÃ©es et dâ□□en retirer un gain personnel. Les utilisateurs privilÃ©giÃ©s qui administrent les systÃ¨mes et les rÃ©seaux reprÃ©sentent dÃ©sormais une inquiÃ©tude supplÃ©mentaire puisque leurs mÃ©tiers requiÃ¨rent Ã©videmment un accÃ¨s Ã toutes les donnÃ©es accessibles sur les systÃ¨mes pour effectuer leur travail.

Â

Une troisiÃ¨me menace intÃ©rieure identifiÃ©e comme Ã©tant particuliÃ¨rement prÃ©occupante concerne les infiltrations par des cybercriminels cherchant activement le moyen de compromettre des comptes dâ□□utilisateurs internes (en visant principalement les comptes avec les privilÃ¨ges les plus avancÃ©s) afin de sâ□□infiltrer dans les systÃ¨mes et dâ□□y voler des donnÃ©es en utilisant les identifiants usurpÃ©s.

Â« *Environ la moitiÃ© des organisations estiment que ces menaces internes sont de plus en plus difficiles Ã dÃ©tecter, et les responsables informatiques sont extrÃªmement inquiets de ce que leurs utilisateurs peuvent faire avec les donnÃ©es de leur entreprise*, dÃ©clare Andrew Kellet, analyste principal chez Ovum, le cabinet dâ□□analystes en charge de lâ□□enquÃªte.

Ce risque se combine avec la menace posÃ©e par les cyberattaques qui visent les comptes utilisateurs â□□ ce qui nâ□□est pas complÃ¨tement ignorÃ© puisque 30 % des organisations citent les Menaces Persistantes AvancÃ©es comme motivation principale pour lâ□□amÃ©lioration des dÃ©fenses contre le vol de donnÃ©es. Â»

Les principaux rÃ©sultats de lâ□□Ã©tude incluent :

â□¢ Seulement 9 % des organisations europÃ©ennes interrogÃ©es se sentent Ã lâ□□abri des menaces internes contre 11% des entreprises franÃ§aises
â□¢ 47 % des organisations estiment actuellement quâ□□il est plus difficile de dÃ©tecter des incidents provenant des menaces internes quâ□□en 2012
â□¢ Le contrÃ´le dâ□□accÃ¨s aux donnÃ©es est identifiÃ© comme la plus grande menace pour les organisations. Pour certaines, les employÃ©s non-techniciens avec un accÃ¨s autorisÃ© aux donnÃ©es sensibles et aux ressources IT reprÃ©sentent le risque le plus important (49 %), tandis que pour dâ□□autres, ce sont les postes de haut niveau tels que les Directeurs Administratifs et Financiers ou les PDG qui sont le principal risque (29 %)

â□¢ Le passage au cloud augmente les risques de sÃ©curitÃ©, en raison dâ□□une perte de visibilitÃ© sur les mesures de sÃ©curitÃ© autour des donnÃ©es stockÃ©es dans le cloud, reprÃ©sentant une inquiÃ©tude pour 62 % des personnes interrogÃ©es
â□¢ Le Big Data peut Ã©galement poser problÃ¨me, avec plus de la moitiÃ© des entreprises concernÃ©es par la sÃ©curitÃ© du Big Data (53 %) indiquant que des donnÃ©es sensibles peuvent y Ãªtre contenues
â□¢ Il y a de bonnes nouvelles : les organisations prennent des mesures pour lutter contre les menaces intÃ©rieures avec 66 % dâ□□entre elles qui envisagent dâ□□augmenter leurs budgets de sÃ©curitÃ© en rÃ©ponse directe Ã ce risque

Â« *Les entreprises accentuent leur utilisation du cloud computing afin de profiter de la flexibilitÃ© et des avantages financiers quâ□□il apporte*, indique Daniele Catteddu, Responsable EMEA pour la Cloud Security Alliance. *Lâ□□Ã©tude dÃ©montre quâ□□elles sont conscientes des nouveaux risques liÃ© Ã cet usage accru, et dÃ©taille la faÃ§on dont les fournisseurs peuvent amÃ©liorer leurs offres afin de mieux satisfaire les besoins des entreprises en matiÃ¨re de sÃ©curitÃ© pour contrebalancer les menaces intÃ©rieures* Â»

Â« *Clairement, les exigences liÃ©es Ã la conformitÃ© lÃ©gale, les contraintes concernant la vie privÃ©e et les vols de donnÃ©es incessants ont un effet marquÃ© sur les entreprises,* dÃ©clare Stewart Room, partenaire du Field Fisher Waterhouse's Technology and Outsourcing Group. *Avec 66% dâ□□entre elles qui envisagent dâ□□augmenter leurs dÃ©penses en sÃ©curitÃ© pour bloquer les menaces intÃ©rieures, et en fonction du dÃ©fi que la protection des donnÃ©es dans le cloud, les environnements mobiles et Big Data reprÃ©sente, les entreprises comprennent que leur niveau de sÃ©curitÃ© doit Ãªtre mis Ã jour et font ce quâ□□il faut pour.* Â»

De plus, les entreprises reconnaissent que le chiffrement est la technologie la plus efficace pour bloquer les menaces internes, avec la plus grande proportion des organisations (38 %) la citant comme la mesure de sÃ©curitÃ© la plus importante.

Â« *MalgrÃ© la frÃ©quence croissante dâ□□incidents liÃ©s aux menaces provenant de lâ□□intÃ©rieur dÃ©crits dans les mÃ©dias, le rapport dÃ©montre que les organisations sont encore aux prÃ©mices de la prise en compte de ces vecteurs de pertes de donnÃ©es*, conclut Alan Kessler, PDG de Vormetric. *Les rÃ©sultats montrent une augmentation de la prise de conscience*

des menaces internes, mais la croissance rapide du volume dâ□□informations sensibles dans une entreprise et lâ□□utilisation de nouvelles technologies comme le cloud et le Big Data, rendent la perspective de sÃ©curiser les donnÃ©es avec un nombre toujours plus grand de solutions ponctuelles, onÃ©reuses et complexes.

Câ□□est un obstacle Ã la mise en place de nouveaux services. Avec ces nouvelles technologies, et avec la croissance des menaces quâ□□elles soient extÃ©rieures ou intÃ©rieures comme les MPA, les protections traditionnelles des postes et du pÃ©rimÃ¨tre rÃ©seau ne sont simplement plus efficaces. Pour se dÃ©fendre efficacement, les entreprises doivent dÃ©velopper une approche data-centrÃ©e, mettre en Å□uvre du chiffrement et des contrÃ´les dâ□□accÃ¨s pour limiter leur exposition, et tracer les accÃ¨s aux donnÃ©es afin dâ□□identifier les activitÃ©s inappropriÃ©es des utilisateurs, en ayant une approche plateforme qui sâ□□Ã©tend en parallÃ¨le avec le nombre croissant dâ□□obligations et de contraintes en termes de protection de donnÃ©es, sans dÃ©tourner une quantitÃ© dÃ©mesurÃ©e des ressources de lâ□□IT. Â»

Pour en savoir plus sur les risques posÃ©s par les menaces internes.