87% des PME franÃ§aises pensent courir un risque, 70% ne changent rien
SÃ©curitÃ©
PostÃ© par : JulieM
PubliÃ©e le : 2/10/2014 13:30:00

Plus de 80% des responsables IT pensent quâ□□un vol de donnÃ©es interne est probable dans leur entreprise, mais environ 60% dÃ©clarent ne pas avoir de procÃ©dure stricte dans ce domaine LogRhythm, spÃ©cialiste de la Security Intelligence, annonce les rÃ©sultats dâ□□une Ã©tude* menÃ©e auprÃ¨s de responsables IT dâ□□entreprises franÃ§aises, Ã propos de leur perception de la sÃ©curitÃ© au sein de leurs entreprises, et notamment des risques en interne.

Dâ□□aprÃ¨s lâ□□enquÃªte, les entreprises franÃ§aises ont bien conscience des dangers liÃ©s au vol de donnÃ©es et des consÃ©quences pour leurs organisations. Toutefois, il semble que les bonnes intentions ne soient pas mises en pratique et quâ□□une remise en question des systÃ¨mes et stratÃ©gies de sÃ©curitÃ© en place ne soit toujours pas Ã lâ□□ordre du jour.

En effet, selon lâ□□Ã©tude, 87% des entreprises franÃ§aises pensent quâ□□elles courent peut-Ãªtre un risque de sÃ©curitÃ© actuellement, dont 34,5% des rÃ©pondants qui en sont persuadÃ©s. Pourtant, 70% des organisations indiquent nâ□□avoir rien changÃ© Ã leurs systÃ¨mes de sÃ©curitÃ© suite aux rÃ©centes affaires de vol de donnÃ©es, alors que 58% dâ□□entre elles se disent plus inquiÃ¨tes sur ce sujet suite aux rÃ©vÃ©lations de Snowden.

Bien que cette derniÃ¨re affaire ait Ã©tÃ© Ã©rigÃ©e en parfait exemple de ce que lâ□□on peut craindre pour les donnÃ©es confidentielles de la part dâ□□employÃ©s ou de partenaires mal intentionnÃ©s, lâ□□Ã©tude rÃ©vÃ¨le que les entreprises y attachent moins dâ□□importance quâ□□aux menaces externes : 52% des rÃ©pondants pensent que les menaces les plus sÃ©rieuses pour les informations confidentielles de leur entreprise viennent de lâ□□extÃ©rieur contre 37% qui jugent les menaces internes comme Ã©tant plus importantes.

Pourtant, les risques associÃ©s sont bien identifiÃ©s : lorsquâ□□on interroge les responsables IT sur la possibilitÃ© que des employÃ©s accÃ¨dent Ã des donnÃ©es sensibles au sein du systÃ¨me dâ□□information, 81% pensent que cela est tout Ã fait probable, dont 23,5% dÃ©clarant que cela Ã©tait dÃ©jÃ arrivÃ©.

Les menaces internes jugÃ©es moins importantes

Si 41,5% des entreprises disposent de procÃ©dures contre le vol de donnÃ©es confidentielles en interne, environ 34,5% des personnes interrogÃ©es pensent que les systÃ¨mes en place ne sont soit pas appliquÃ©s, soit pas satisfaisants. 15% ne savent mÃªme pas si ce type de procÃ©dure existe dans leur entreprise et 9% confirment ne pas en avoir du tout. Parmi ces derniers exempts de tout contrÃ´le de sÃ©curitÃ©, 15% des personnes interrogÃ©es pensent que cela nâ□□est tout simplement Â« pas nÃ©cessaire Â».

En ce qui concerne les procÃ©dures de sÃ©curitÃ© Ã©lÃ©mentaires, lâ□□Ã©tude montre quâ□□environ 30% des personnes interrogÃ©es ne procÃ¨dent toujours pas au renouvellement de leurs mots de passe. Parmi eux, il y a ceux qui savent que câ□□est nÃ©cessaire mais qui ne le font pas (24%) mais aussi 5,5% des rÃ©pondants qui estiment que cela ne sert Ã rien !

Â« *Les entreprises franÃ§aises sont sensibilisÃ©es aux risques majeurs de sÃ©curitÃ© mais les bonnes pratiques ne sont toujours pas appliquÃ©es*, confie Jean-Pierre Carlin, Directeur Europe du Sud chez LogRhythm. *Les donnÃ©es des entreprises ne sont peut-Ãªtre pas aussi critiques que celles de la NSA, il nâ□□en reste pas moins Ã©tonnant que les employÃ©s ne soient pas plus impliquÃ©s par la direction sur cette pratique essentielle pour la sÃ©curitÃ© de leurs donnÃ©es*

alors que la menace est bien rÃ©elle. Il est trÃ¨s surprenant que des procÃ©dures aussi basiques que le renouvellement rÃ©gulier de mot de passe ne soient pas encore systÃ©matiquement appliquÃ©es. Â»

Selon cette Ã©tude, le manque dâ□□information, mais aussi dâ□□implication de la part des directions Ã se saisir de ces problÃ©matiques, engendre une sorte de laisser-aller sur la question de lâ□□accÃ¨s aux donnÃ©es, surtout en interne. MalgrÃ© les inquiÃ©tudes justifiÃ©es, les stratÃ©gies et procÃ©dures en place restent insuffisantes Ã ce jour.

La formation des employÃ©s, lâ□□application systÃ©matique des bonnes pratiques liÃ©es au contrÃ´le dâ□□accÃ¨s et Ã la gestion des mots de passe est aujourdâ□□hui indispensable pour initier une vraie stratÃ©gie de sÃ©curitÃ© des donnÃ©es. Sans compter que ces mesures doivent elles-mÃªmes Ãªtre complÃ©tÃ©es par dâ□□autres procÃ©dures rÃ©gissant lâ□□ensemble des questions relatives Ã la protection des ressources de lâ□□entreprise, que ce soit en matiÃ¨re de contrÃ´le dâ□□accÃ¨s, ou de sanction des employÃ©s en cas de manquement ou de mauvaise application des rÃ¨gles de sÃ©curitÃ©.