Les collaborateurs, premiÃ¨re menace pour les donnÃ©es de lâ□□entreprise ?
Accessoire
PostÃ© par : JPilo
PubliÃ©e le : 22/6/2015 13:30:00

Selon une rÃ©cente Ã©tude rÃ©alisÃ©e en France, les salariÃ©s seraient trÃ¨s confiants quant Ã la sÃ©curitÃ© informatique au sein de leur entreprise. En effet, seuls 36% dâ□□entre eux pensent quâ□□elle a dÃ©jÃ Ã©tÃ© la cible de hackers alors quâ□□en rÃ©alitÃ©, 90% des organisations reconnaissent avoir dÃ©jÃ subi une attaque.

En outre, 85% des personnes interrogÃ©es estiment que leur entreprise est bien protÃ©gÃ©e contre les cyber-attaques et les hackers. Des rÃ©sultats qui rÃ©vÃ¨lent une importante contradiction entre la perception des employÃ©s et la rÃ©alitÃ© des risques actuels qui planent sur les ressources et les donnÃ©es dâ□□une organisation alors que les menaces se multiplient et sont de plus en plus sophistiquÃ©es.

Ces chiffres sont surprenants dans la mesure oÃ¹ les affaires de faille de sÃ©curitÃ© et de vol de donnÃ©es massifs font trÃ¨s rÃ©guliÃ¨rement la une des mÃ©dias depuis quelques mois.

Ce sentiment de confiance reprÃ©sente une vÃ©ritable porte ouverte aux hackers car si les collaborateurs nâ□□ont pas conscience des risques qui planent sur les donnÃ©es et les ressources de lâ□□entreprise, il y a fort Ã parier pour que les bonnes pratiques et les procÃ©dures essentielles en matiÃ¨re de sÃ©curitÃ© ne soient pas non plus appliquÃ©es, voire nÃ©gligÃ©es.

En outre, ce nâ□□est pas parce quâ□□une entreprise est protÃ©gÃ©e quâ□□elle ne subira pas dâ□□attaque, ce que semblent pourtant penser les employÃ©s interrogÃ©s. En effet, des hackers qui souhaitent pÃ©nÃ©trer au sein dâ□□un systÃ¨me dâ□□information finiront tÃ´t ou tard par y parvenir, mÃªme si cela prend du temps.

Pour que les collaborateurs aient une perception en adÃ©quation avec la rÃ©alitÃ©, les entreprises doivent impÃ©rativement poursuivre leurs efforts pour les sensibiliser aux cyber-risques, aussi bien pour leurs donnÃ©es personnelles que pour celles de lâ□□organisation, ainsi quâ□□aux consÃ©quences prÃ©judiciables que peut entrainer une fuite de donnÃ©es.

La formation de lâ□□ensemble des membres dâ□□une organisation aux risques, aux diffÃ©rents types dâ□□attaques potentielles ainsi quâ□□Ã lâ□□application systÃ©matique des bonnes pratiques reprÃ©sentent la base pour initier une stratÃ©gie globale de sÃ©curitÃ© efficace. Le contrÃ´le dâ□□accÃ¨s, la vigilance relative aux emails ainsi que le renouvellement rÃ©gulier des mots de passe font notamment partie des mesures indispensables.

En outre, les responsables de la sÃ©curitÃ© doivent mettre en place un dispositif de sanction pour les employÃ©s qui ne respectent pas les rÃ¨gles imposÃ©es par lâ□□entreprise, pour une meilleure implication mais aussi pour engager leur responsabilitÃ©.

Selon lâ□□Ã©tude Capgemini, 28% des personnes interrogÃ©es estiment que la politique de sÃ©curitÃ© informatique de leur sociÃ©tÃ© nâ□□est pas vraiment claire, voire pas du tout, et 39% dÃ©clarent ne pas la connaÃ®tre. Ces rÃ©sultats rÃ©vÃ¨lent un manque dâ□□information et peut-Ãªtre un manque dâ□□implication de la part des directions Ã se saisir de ces problÃ©matiques auquel les entreprises doivent rapidement remÃ©dier.

Pour les entreprises qui ne possÃ¨dent pas forcÃ©ment les ressources en interne (un CSO par

exemple, responsable principal de la sÃ©curitÃ©), lâ□□Agence Nationale de la SÃ©curitÃ© des SystÃ¨mes dâ□□Information (ANSSI) et la ConfÃ©dÃ©ration GÃ©nÃ©rale du Patronat des Petites et Moyennes Entreprises (CGPME) ont publiÃ© en mars dernier un guide des bonnes pratiques pour les PME.

Cette excellente initiative rÃ©pond Ã lâ□□urgente nÃ©cessitÃ© de sensibiliser les salariÃ©s aux consÃ©quences qui peuvent rÃ©sulter dâ□□une simple nÃ©gligence et des rÃ¨gles de base Ã respecter, et aide les organisations en leur proposant une expertise adaptÃ©e Ã leurs besoins. Nous les encourageons donc vivement Ã partager ce guide en marge de leur stratÃ©gie globale de sÃ©curitÃ© pour une meilleure information, prÃ©vention et prise de conscience des risques qui conduiront Ã lâ□□adoption des bons rÃ©flexes.

La contradiction entre la perception de la cyber-sÃ©curitÃ© par les salariÃ©s et la rÃ©alitÃ© met en avant le fait que lâ□□humain reste lâ□□un des maillons faibles dâ□□une organisation. Les hackers le savent trÃ¨s bien, câ□□est la raison pour laquelle ils sont Ã lâ□□affÃ»t du moindre faux pas. Dans ce contexte, la protection des donnÃ©es et des ressources reprÃ©sente aujourdâ□□hui un vÃ©ritable dÃ©fi pour les entreprises.

Il est donc primordial de faire prendre conscience aux employÃ©s que les cyber-risques sont rÃ©els, que les attaques ne sont pas uniquement portÃ©es sur les grandes organisations connues, et quâ□□ils peuvent eux-mÃªmes en Ãªtre Ã lâ□□origine.

Avec une plus grande implication de la direction gÃ©nÃ©rale pour la formation de lâ□□ensemble des collaborateurs, associÃ©e aux initiatives des autoritÃ©s rÃ©gissant la sÃ©curitÃ© informatique, les entreprises vont pouvoir renforcer la protection de leurs donnÃ©es ainsi que lâ□□efficacitÃ© de leur politique de sÃ©curitÃ©, un enjeu majeur Ã lâ□□heure oÃ¹ les cyber-attaques sont devenues monnaie courante, commente Jean-Pierre Carlin, Directeur Europe du Sud chez LogRhythm.