Les documents papier prÃ©sentent un risque pour les PME
SÃ©curitÃ©
PostÃ© par : JPilo
PubliÃ©e le : 7/9/2012 11:30:00

Dans lâinconscient collectif, lâespionnage industriel fait penser Ã tout un monde de gadgets high-tech et dâagents du renseignement, vÃªtus dâimpermÃ©able, luttant contre le crime organisÃ©. Nous voici bien loin du quotidien du bureau, nâest-ce pas ?, nous explique **Marc Delhaie**, PrÃ©sident-Directeur GÃ©nÃ©ral dâIron Mountain France

Pour faire simple, lâespionnage industriel ou Ã©conomique se dÃ©finit par le fait dâobtenir des informations sur une entreprise, dâune faÃ§on illÃ©gale ou contraire Ã lâÃ©thique. Les entreprises doivent aujourdâhui se dÃ©fendre en permanence contre les tentatives dâintrusion de tiers souhaitant accÃ©der Ã leurs informations depuis lâextÃ©rieur. Pour construire une forteresse numÃ©rique tout autour de leurs donnÃ©es, elles nâhÃ©sitent pas Ã investir lourdement dans lâinformatique. En 2011, par exemple, les gouvernements, lâindustrie et les particuliers Ã©quipÃ©s en informatique ont dÃ©pensÃ© quelque 83 milliards dâeuros dans des solutions et services de protection contre les menaces externes ; un chiffre qui devrait doubler au cours des 5 prochaines annÃ©es.

Mais comme je viens de lâindiquer, lâespionnage Ã©conomique recouvre de multiples activitÃ©s, qui ne sont pas toutes manifestement criminelles ou forcÃ©ment malveillantes. Il existe de multiples catÃ©gories dâinformation et autant de moyens de se les procurer. La responsabilitÃ© de la gestion de lâinformation revenant le plus souvent aux services informatiques, lâattention et les budgets sont allouÃ©s Ã la maintenance et la consolidation des systÃ¨mes informatiques. Conclusion : les entreprises mÃ©sestiment le risque que prÃ©sentent les documents papier et perdent de vue la gravitÃ© des menaces auxquelles leurs employÃ©s les exposent, souvent inintentionnellement.

Une Ã©tude rÃ©cente dâIron Mountain rÃ©vÃ¨le que les employÃ©s de bureau se fient souvent Ã leur bon sens pour dÃ©terminer sâils peuvent ou non manipuler les informations confidentielles et sensibles de leur employeur. Faute de politique clairement Ã©tablie, ils dÃ©cident eux-mÃªmes des pratiques qui leur semblent acceptables. Les rÃ©sultats de lâÃ©tude vis-Ã -vis de lâaccÃ¨s aux informations de la concurrence sont dâailleurs

particuliÃ¨rement intÃ©ressants.

Lâ□□initiÃ© en situation dâ□□espionnage Ã©conomique est souvent prÃ©sentÃ© comme lâ□□employÃ© qui sort des informations de lâ□□entreprise, plutÃ´t que celui qui fait rentrer des informations. La liste des profils dâ□□initiÃ©s Ã©tablie par Securelist pour aider les entreprises Ã identifier les groupes Ã haut risque et les comprendre, rÃ©pertorie ainsi 4 catÃ©gories : Â« lâ□□initiÃ© nÃ©gligent Â», le type le plus frÃ©quent, le plus souvent un exÃ©cutant qui laisse fuiter des informations accidentellement ; Â« lâ□□initiÃ© naÃ¯f Â», qui rÃ©pond sans se mÃ©fier Ã des Ã©tudes de marchÃ© intÃ©ressÃ©es ou dâ□□autres escroqueries procÃ©dant par abus de confiance ; et ceux qui organisent dÃ©libÃ©rÃ©ment la fuite dâ□□information, y compris le Â« saboteur Â», souvent un employÃ© mÃ©content qui se sent lÃ©sÃ©, et Â« lâ□□initiÃ© dÃ©loyal Â», qui envisage gÃ©nÃ©ralement de quitter rapidement lâ□□entreprise.

Les politiques internes de gestion de lâ□□information doivent absolument tenir compte de chacune de ces catÃ©gories de risque, mais comment procÃ©der avec les employÃ©s qui font rentrer des informations confidentielles ? Dans son Ã©tude, Iron Mountain rÃ©vÃ¨le que plus de la moitiÃ© des employÃ©s interrogÃ©s (53 %), feraient volontiers part des informations recueillies Ã leur employeur.

Lâ□□analyse des rÃ©ponses obtenues nous apprend que beaucoup parmi les sondÃ©s seraient surpris dâ□□Ãªtre accusÃ©s de comportement indigne. De plus, ils seraient nombreux Ã considÃ©rer que la faute revient Ã lâ□□entreprise, trop nÃ©gligente dans la protection de ses informations confidentielles. Iron Mountain a souhaitÃ© savoir quel comportement les employÃ©s de bureau sondÃ©s adopteraient, en Europe, sâ□□ils dÃ©couvraient par hasard des informations confidentielles sur un concurrent.

Les rÃ©ponses obtenues rÃ©vÃ¨lent des disparitÃ©s frappantes entre les 4 pays europÃ©ens Ã©tudiÃ©s. Par exemple, plus des 2/3 (69 %) des employÃ©s en France nâ□□hÃ©siteraient pas Ã rÃ©vÃ©ler des informations confidentielles sâ□□ils en avaient lâ□□occasion, contre 57 % en Espagne, 50 % au Royaume-Uni et seulement 33 % en Allemagne. Les employÃ©s de bureau allemands sont ceux qui rechignent le plus Ã communiquer des informations obtenues accidentellement, puisquâ□□ils sont moins dâ□□1/3 des sondÃ©s (32 %) Ã lâ□□envisager, contre 51 % au Royaume-Uni, 61 % en France et 63 % en Espagne.

Une conclusion trÃ¨s intÃ©ressante sâ□□impose Ã la comparaison des rÃ©sultats de lâ□□Ã©tude : le comportement des employÃ©s est directement liÃ© Ã la politique de protection des donnÃ©es de lâ□□entreprise et Ã la maniÃ¨re dont elle leur est communiquÃ©e. Ainsi, les sondÃ©s allemands sont de loin les plus nombreux Ã indiquer que les informations confidentielles sont clairement estampillÃ©es comme telles dans leur entreprise (67 % des employÃ©s, contre 56 % au Royaume-Uni et en Espagne et seulement 49 % en France) et ils sont 80 % Ã dÃ©clarer connaÃ®tre les consignes de leur entreprise vis-Ã -vis des informations quâ□□il est ou non possible de sortir de lâ□□entreprise, 66 % au Royaume-Uni et un peu plus de la moitiÃ© des sondÃ©s en France et en Espagne (57 et 56 %.)

Voici ce quâ□□il faut retenir : les mesures mises en place pour Ã©viter toute fuite des informations confidentielles et sensibles de lâ□□entreprise semblent inciter les employÃ©s Ã adopter un code de conduite quâ□□ils appliquent dâ□□emblÃ©e aux informations appartenant Ã des tiers.

La frontiÃ¨re entre comportement Ã©thique et contraire Ã lâ□□Ã©thique est, et restera floue. La curiositÃ© est un penchant naturel qui, au mieux, stimule la crÃ©ativitÃ© et la motivation. Quâ□□un employÃ© soit fascinÃ© par les secrets de la concurrence peut signifier sa loyautÃ© envers son employeur et son intÃ©rÃªt pour son secteur dâ□□industrie. Sâ□□il nous serait difficile de ne pas jeter un Å□il Ã la prÃ©sentation Powerpoint que visionne votre voisin dans le train, salariÃ© dâ□□une sociÃ©tÃ© concurrente, ou dâ□□ignorer la conversation dâ□□employÃ©s dâ□□un

concurrent faisant une pause devant la machine cafÃ© entre deux sessions de confÃ©rence, la plupart dâentre nous refuseraient dâentrer par effraction dans les locaux dâune entreprise pour copier ou voler des informations confidentielles. Mais entre ces deux extrÃªmes, finalement, seul notre propre code moral peut nous guider. Des consignes claires de gestion de lâinformation semblent aider les employÃ©s Ã dÃ©finir ce code.

En dâautres termes, les directives de gestion de lâinformation les plus efficaces ne sont pas simplement celles qui protÃ¨gent physiquement lâinformation en contrÃ´lant les conditions de stockage, de distribution, dâaccÃ¨s, de sÃ©curitÃ© et de destruction, voire mÃªme celles qui sensibilisent les employÃ©s aux risques de divulguer des informations par inadvertance. Non, ce sont celles qui encouragent les employÃ©s Ã considÃ©rer les informations de leur entreprise avec un sentiment de fiertÃ©, de propriÃ©tÃ© et de responsabilitÃ©.