La difficultÃ© croissante des directions informatiques Ã protÃ©ger leur PME
SÃ©curitÃ©
PostÃ© par : JPilo
PubliÃ©e le : 8/10/2014 13:30:00

Les dÃ©cisions de sÃ©curitÃ© des entreprises gagnent les directions gÃ©nÃ©rales et deviennent un critÃ¨re clÃ© des projets dâentreprise. 90% (81% en France) des DSI et Directeurs Informatiques estiment que la protection de leurs entreprises est une mission de plus en plus difficile, selon une nouvelle Ã©tude, lâun des leaders mondial de la sÃ©curitÃ© rÃ©seau haute-performance.

La forte pression Ã©manant des directions gÃ©nÃ©rales pour sÃ©curiser leur entreprise a augmentÃ© au cours des 12 derniers mois (de prÃ¨s dâun tiers pour le panel mondial et de 11% en France), faisant de la sÃ©curitÃ© une prioritÃ© et une prÃ©occupation clÃ© sur les autres projets de lâentreprise.

Cet Ã©tat des lieux rÃ©sulte dâune enquÃªte indÃ©pendante commanditÃ©e par Fortinet sur plus de 1600 dÃ©cideurs informatiques, en grande partie dâentreprises de plus de 500 collaborateurs. Toutes les personnes interrogÃ©es provenaient du panel en ligne de lâentreprise dâÃ©tude de marchÃ© Lightspeed GMI.

Les principaux enseignements de cette Ã©tude sont :

- Parmi les dÃ©cideurs IT qui subissent la pression la plus Ã©levÃ©e de la part de leur direction, 63% (52% en France) dÃ©clarent avoir abandonnÃ© ou retardÃ© au moins un nouveau projet mÃ©tier en raison des prÃ©occupations liÃ©es Ã la sÃ©curitÃ© informatique.

- Les plus grands dÃ©fis rencontrÃ©s par les dÃ©cideurs IT pour garder leurs entreprises sÃ©curisÃ©es sont les menaces toujours plus complexes et frÃ©quentes (citÃ©es par 88% du panel mondial) et les nouveaux besoins liÃ©s aux technologies Ã©mergentes de type Internet des Objets et biomÃ©trie (88% du panel mondial). En France, les menaces toujours plus complexes et frÃ©quentes (85%) et les besoins liÃ©s au BYOD et Ã la mobilitÃ© des salariÃ©s (82%) sont les plus grands dÃ©fis rencontrÃ©s par les dÃ©cideurs IT franÃ§ais.

- La majoritÃ© des dÃ©cideurs IT a Ã©tÃ© incitÃ©e Ã prendre des mesures pour assurer la confidentialitÃ© des donnÃ©es (90% au niveau mondial et franÃ§ais) et sÃ©curiser le Big Data (89% du panel mondial et 88% en France). Dans la majoritÃ© des cas, ces initiatives ont abouti Ã de nouveaux investissements en sÃ©curitÃ© au niveau mondial tandis quâen France, cela conduit Ã repenser la stratÃ©gie de sÃ©curitÃ© de lâentreprise.

Les directions gÃ©nÃ©rales donnent la prioritÃ© Ã la sÃ©curitÃ©

La prise de conscience qui sâopÃ¨re au niveau des directions gÃ©nÃ©rales vis-Ã -vis de la sÃ©curitÃ© informatique - et les pressions et implications qui en dÃ©coulent - est citÃ©e comme important vecteur de complexitÃ© dans le travail des dÃ©cideurs IT. Les trois-quarts des personnes interrogÃ©es (77% en France) Ã©valuent la prise de conscience de leurs dirigeants comme â Ã©levÃ©eâ ou â trÃ¨s Ã©levÃ©eâ, contre seulement 50% (51% en France) il y a un an.

Lâenquête révèle également que 53% (45% en France) des décideurs IT interrogés déclarent avoir ralenti ou abandonné un projet de nouvelle application, de nouveau service ou autre, par crainte de cyber-menaces. Ce chiffre monte Ã 63% (52% en France) pour ceux qui déclarent subir une très forte pression de leur direction générale en matière de sécurité IT.

Les applications et stratÃ©gies de mobilitÃ© sont les initiatives qui sont estimÃ©es comme les plus problÃ©matiques, suivies par celles liÃ©es au cloud au niveau mondial et en France.

Les prÃ©occupations en matiÃ¨re de sÃ©curitÃ© sâ□□intensifient avec les technologies Ã©mergentes

Pour 88% du panel mondial, la mission des dÃ©cideurs IT devient plus difficile du fait de la complexitÃ© et la recrudescence des menaces APT, attaques DDoS et autres cyber menaces, ainsi que des nouvelles tendances technologiques telles que lâ□□Internet des Objets (Internet of Things ou IoT) et la biomÃ©trie. En France, les menaces toujours plus complexes et frÃ©quentes (85%) et les besoins liÃ©s au BYOD et la mobilitÃ© des salariÃ©s (82%) sont les plus grands dÃ©fis rencontrÃ©s par les dÃ©cideurs IT franÃ§ais.

Les attentes sont fortes, dans tous les secteurs dâ□□activitÃ©, vis-Ã -vis de la biomÃ©trie, avec 46% des rÃ©pondants qui dÃ©clarent que cette technologie est dÃ©jÃ dâ□□actualitÃ© dans leur entreprise, ou le sera au cours des 12 prochains mois contre seulement 29% en France.

Deux tiers des personnes interrogÃ©es estiment dÃ©jÃ disposer des outils qui permettront de gÃ©rer la biomÃ©trie en toute sÃ©curitÃ© (contre 56% en France). Parmi le tiers (44% en France) des rÃ©pondants qui estiment aujourdâ□□hui ne pas avoir les outils prÃªts pour sÃ©curiser la biomÃ©trie, un tiers du panel mondial et franÃ§ais estime quâ□□ils rencontreront des difficultÃ©s pour le sÃ©curiser dans le futur.

La sÃ©curitÃ© du Big Data et la confidentialitÃ© des donnÃ©es conduisent Ã une autre approche

Les problÃ©matiques en matiÃ¨re de confidentialitÃ© des donnÃ©es incitent Ã un plan dâ□□actions, avec 90% des dÃ©cideurs IT mondiaux et franÃ§ais qui pensent faire Ã©voluer leur approche en matiÃ¨re de stratÃ©gie de sÃ©curitÃ©. Parmi eux, 56% (50% en France) sont enclins Ã investir davantage en ressources financiÃ¨res et humaines pour rÃ©pondre Ã ces dÃ©fis, tandis que 44% (50% en France) dÃ©clarent plutÃ´t vouloir repenser leur stratÃ©gie existante.

Le Big Data et le traitement analytique des donnÃ©es sont considÃ©rÃ©s par 89% des rÃ©pondants comme un facteur de changement dâ□□approche en matiÃ¨re de stratÃ©gie de sÃ©curitÃ© informatique, et incitent 50% des rÃ©pondants Ã planifier de nouveaux investissements. En France, 88% des rÃ©pondants pensent que le Big Data est un facteur de changement dâ□□approche en matiÃ¨re de stratÃ©gie de sÃ©curitÃ© informatique, incitant 40% Ã prÃ©voir de nouveaux investissements.

Les secteurs dâ□□activitÃ© les plus enclins Ã investir dans la sÃ©curitÃ© informatique sont les services financiers (53%) et celui des technologies/tÃ©lÃ©communications (59%). En France, les entreprises issues des technologies/tÃ©lÃ©communications (75%) et de la distribution (67%) sont les secteurs dâ□□activitÃ© les plus enclins Ã investir dans la sÃ©curitÃ© informatique. Lâ□□Ã©tude souligne Ã©galement que ce sont les plus grandes organisations qui sont les plus susceptibles dâ□□investir.

InterrogÃ©s sur le fait dâ□□avoir obtenu suffisamment de ressources humaines et financiÃ¨res pour la sÃ©curitÃ© informatique au cours des 12 derniers mois, quatre dÃ©cideurs sur 5 rÃ©pondent positivement (75% en France). Dâ□□autre part, 83% (73% en France) des rÃ©pondants estiment que ces ressources seront suffisantes au cours des 12 prochains mois.

La majoritÃ© des secteurs dâ□□activitÃ© sâ□□inscrit dans cette tendance, avec, par exemple : 74% (au cours des 12 derniers mois) et 77% (pour lâ□□annÃ©e Ã venir) dans le secteur public et respectivement 80% et 81% dans la distribution. Les services financiers sont les mieux lotis (87% pour les 12 prochains mois), en dÃ©pit dâ□□un lÃ©ger flÃ©chissement (89% au cours des 12 mois

prÃ©cÃ©dents) au niveau mondial.

En France, seul le secteur de la construction et de lâ□□industrie sâ□□inscrit dans cette tendance passant de 66% (au cours des 12 derniers mois) Ã 74% (pour lâ□□annÃ©e Ã venir). Les secteurs des technologies/tÃ©lÃ©communications, de la distribution et des services financiers sâ□□attendent Ã avoir autant de ressources financiÃ¨res et humaines quâ□□au cours des 12 derniers mois. Le secteur public ainsi que celui de la grande consommation sont en dÃ©clins en passant respectivement de 73% Ã 53% et de 100% Ã 50%.

Un rÃ©el besoin de cyber-rÃ©silience

â□□*Alors que la sÃ©curitÃ© IT devient une prioritÃ© pour les dirigeants, elle reste nÃ©anmoins associÃ©e Ã dâ□□autres challenges qui pÃ¨sent lourdement sur les professionnels de lâ□□informatique et remettent en cause la capacitÃ© de certaines organisations Ã innover tout en assurant leur sÃ©curitÃ©*â□□, explique Patrice Perche, Senior Vice PrÃ©sident, en charge des opÃ©rations commerciales et de support Ã lâ□□international chez Fortinet.

â□□*Ces organisations doivent agir dÃ¨s aujourdâ□□hui pour maÃ®triser lâ□□impact de menaces en forte croissance et se focaliser davantage sur la sÃ©curitÃ© IT afin de renforcer leur rÃ©silience face aux cybermenaces* Â».

Â« *La bonne nouvelle est que nombre dâ□□entreprises restent optimistes et sâ□□estiment bien armÃ©es en matiÃ¨re de ressources financiÃ¨res et humaines pour face aux dÃ©fis de sÃ©curitÃ© informatique Ã venir. Mais au-delÃ de ces investissements, elles doivent repenser leur stratÃ©gie de sÃ©curitÃ© informatique et considÃ©rer de nouvelles technologies de sÃ©curitÃ© IT.* Â»