Les mégas vols de données n'impressionnent pas l'IT

L'enquête trimestrielle du cabinet américain 451 Research sur la sécurité de l'information a été réalisée auprès d'un panel de plus de 900 décideurs IT d'Amérique du Nord et d'Europe, essentiellement. Malgré les cyberattaques d'ampleur comme celles dont ont été victimes Sony Pictures Entertainment, Target et Anthem ou encore l'OPM américain, **67,8 %** des répondants déclarent **ne pas avoir effectué de changement dans leurs dépenses de securité IT**. Et les politiques américaines et européennes visant à intensifier l'échange sur les incidents de sécurité informatique entre entreprises et autorités, n'y changent rien… pour le moment.

Le budget consacré à la sécurité informatique est noyé dans les dépenses IT pour près de 57 % des répondants. 54,5 % disent que leur organisation n'a pas vraiment de responsable de la sécurité SI (**RSSI**). Dans ce contexte, la majorité (51,5 %) pense que les dépenses de sécurité IT ne devraient pas évoluer dans les prochains mois. Malgré les impératifs liés à la gestion des risques et la conformité.

Les hackers ou les initiés

En septembre, rappelle Zdnet.com, la société de conseil financier R.T. Jones, qui a perdu les données sensibles d'au moins 100 000 personnes après l'intrusion d'un tiers dans ses bases de données, a pourtant écopé d'une amende symbolique de 75 000 dollars. Et ce pour ne pas avoir appliqué en amont de l'incident les règles de cybersécurité (Regulation S-P) qui s'imposaient, selon le gendarme boursier américain (SEC). Le régulateur américain du commerce (FTC), de son côté, poursuit Wyndham Hotels. Le groupe hôtelier est accusé de ne pas avoir investi suffisamment dans la sécurité informatique après avoir constaté que 600 000 dossiers de clients ont été exposés en 2008 et 2009.

Mais ces incidents semblent encore peu soucier les décideurs IT interrogés au troisième trimestre 2015, même s'ils pensent à de potentielles attaques informatiques. Devant l'espionnage d'initiés (cité par 17,9 % des répondants) et la cyberguerre (11,7 %), les intentions malveillantes de **hackers/crakers** (21,5 %) constituent la principale inquiétude des répondants. Pourtant, ils ne sont plus que 41,5 % à s'en soucier, alors qu'ils étaient 52,1 % à s'inquiéter au deuxième trimestre.

Lire aussi :
Ingénierie sociale : les employés sont-ils le maillon faible de la cybersécurité ?
Directive NIS : ce que l'Europe prépare pour les acteurs du Web