Sécurité : pourquoi les RSSI peinent à justifier les budgets

Les failles de cybersécurité et violations de données se multiplient. Mais les (RSSI) peinent à recruter, voire à s'imposer dans les conseils d'administration. C'est ce que montre une enquête réalisée par le cabinet PAC pour l'éditeur de logiciels Kaspersky Lab.

250 responsables de la sécurité IT ont été interrogés dans le monde. (Source : *The Chief Information Security Officer Survey 2018*).

Les réseaux cybercriminels aux motivations financières (pour 40% des répondants) et les attaques d'initiés (29%) sont considérés comme les principaux risques. Le cloud dans l'ombre de l'IT et l'usage incontrôlé des réseaux sociaux sont d'autres sujets d'inquiétude.

Face à la mutiplication des menaces et à l'élargissement de la surface d'attaque, 86% des RSSI (80% en Europe) jugent les violations de sécurité informatique « inévitables ». Or, 62% peinent à recruter des professionnels qualifiés pour mieux gérer le risque.

En cause : une pénurie de compétences en sécurité informatique sur certains marchés et la guerre des talents que se livrent les entreprises.

RSSI dans le processus de décision

Les responsables de la sécurité ont-ils l'approbation des directions générales ?

58% des RSSI déclarent être impliqués dans les sphères de décision de leur organisation. Toutefois, seuls 26% font partie du conseil d'administration.

Lorsqu'il est question de négocier les budgets, les RSSI peuvent se trouver en difficulté. Ainsi, plus d'un tiers disent qu'ils luttent pour obtenir les budgets requis.

Et ce pour plusieurs raisons.

En effet, ils ne peuvent garantir un retour sur investissement (ROI) précis ou une protection à 100% contre les cyberattaques. De surcroît, ils entrent en concurrence avec d'autres départements, y compris les opérations IT, sur les questions budgétaires.

Malgré tout, 59% des responsables de la sécurité des systèmes d'information interrogés (49% en Europe) prévoient une augmentation de leurs budgets en 2019.

(crédit photo © shutterstock)