Les entreprises démunies face aux cyberattaques sophistiquées

Le cabinet d'audit EY publie l'édition 2015 de son enquête sur la sécurité de l'information menée entre juin et septembre auprès de **1755 DSI, RSSI et dirigeants d'entreprise** dans 67 pays. L'an dernier, 56 % des répondants déclaraient avoir confiance en leur capacité à détecter des cyberattaques sophistiquées, ils ne sont plus que 36 % à le penser désormais.

Ils redoutent en priorité les menaces d'organisations criminelles (pour 59 % des professionnels interrogés, un taux en hausse de 5 points par rapport à 2014), mais aussi d'employés mal-avisés ou bernés par les techniques d'ingénierie sociale (56 %). Ces derniers devancent même les hacktivistes (54 %), le hacker solitaire (43 %) et les groupes parrainés par des États (35 %).

Opter pour une « défense active »

Globalement, 88 % des répondants pensent que leur système d'information ne répond pas pleinement aux besoins de sécurité de leur entreprise. Et 69 % jugent que le budget de sécurité IT devrait être augmenté jusqu'à 50 % pour assurer un niveau de protection en adéquation avec la politique de gestion du risque de leur entreprise. EY, qui prêche pour sa paroisse, recommande aux entreprises d'investir dans une *« défense active »* (priorisation des actifs, intégration d'un centre des opérations de sécurité ou SOC, gestion avancée des menaces, etc.).

Lire aussi :

Ingénierie sociale : les employés sont-ils le maillon faible de la cybersécurité ?

crédit photo © wk1003mike / shutterstock