

Sécurité de l'information : le pouvoir d'arbitrage des RSSI progresse

Le Club de la sécurité de l'information français (Clusif) publie l'édition 2018 de son [rapport](#) sur les menaces informatiques et pratiques de sécurité (MIPS) en France.

L'enquête a été réalisée cette année auprès de 200 établissements de santé et de 350 entreprises de 100 à plus de 2000 salariés.

Premier constat : le RSSI prend de l'ampleur. Mais les budgets consacrés à la sécurité des systèmes d'information (SSI) stagnent par rapport 2016. En conséquence, la « maturité SSI » des organisations évolue peu. Principalement du fait du manque de budget (pour 36% des répondants). Elles sont aussi impactées par des contraintes organisationnelles (29%), indique le Clusif dans son rapport publié tous les deux ans.

Malgré tout, le nombre d'entreprises ayant formalisé une politique de sécurité des systèmes d'information (PSSI) progresse. 75% l'on fait (+6 points par rapport à 2016 à périmètre comparable). Toutefois ce chiffre n'est plus que de 69% lorsque l'on considère le nouveau périmètre (à savoir la prise en compte d'entreprises de 100 à 200 salariés).

Autre enseignement du rapport : la direction des systèmes d'information (DSI) reste prépondérante dans la formalisation de la PSSI (52%). Elle devance même le responsable de la sécurité des systèmes d'information (RSSI) dans ce domaine (43%).

Mais le responsable de la sécurité des SI monte en grade.

Rattachement du RSSI

85% des banques et 80% des établissements de santé ont un RSSI. En revanche, la fonction est en repli dans d'autres secteurs. Globalement, 63% des entreprises interrogées déclarent avoir pourvu la fonction, soit 4 points de moins par rapport à 2016.

Malgré tout, le « pouvoir d'arbitrage » des RSSI progresse. Près d'un sur deux (49%) est rattaché à la direction générale, 30% à la DSI, selon le Clusif. Des taux bien différents à ceux publiés l'an dernier par [le CESIN](#) (Club des experts de la sécurité de l'information et du numérique).

Il n'empêche, les deux organisations jugent que le RSSI gagne en légitimité. « L'importance de son rôle commencerait-elle à être (mieux) comprise par les directions générales ? », s'interroge le Clusif. Elle l'est sans doute, mais lorsque la cryptographie est utilisée (par 30% des organisations seulement), c'est la DSI qui en a le contrôle (72%).

Tous sont impliqués dans la mise en conformité au Règlement général sur la protection des données ([RGPD](#)). Entré en vigueur le 25 mai, celui-ci mobilise de nombreuses ressources. 68% des entreprises se sont déclarées prêtes, dont 46% partiellement.

Les établissements de santé sont concernés eux aussi. Ils doivent également s'adapter à un cadre

réglementaire en évolution ([PGSSI-S](#), Certification des comptes...). Pour le pilotage de la sécurité de l'information, ils s'appuient surtout sur des normes ou des référentiels.

En conséquence, le nombre d'établissements de santé ayant formalisé leur PSSI a très fortement augmenté, passant de 50% en 2014 à 92% en 2018. De surcroît, « le gestionnaire des risques (IT) est principalement le RSSI ». Un bémol : ces établissements peinent encore à bien évaluer les coûts liés à la sécurité de l'information (pour 81% des répondants).

(crédit photo © Shutterstock)