Cybersécurité : la DSI veut impliquer les métiers

Pour les directions des systèmes d'information, la cybersécurité implique désormais l'ensemble des collaborateurs et s'inscrit dans le cadre d'une politique globale de gestion des risques. C'est ce qui ressort d'un rapport du cabinet de recrutement spécialisé Robert Half. L'enquête s'appuie sur les résultats d'un sondage réalisé auprès de 100 DSI français par un institut indépendant.

75 % des DSI interrogés pensent que les dirigeants comprennent bien les risques de cybersécurité auxquels leur organisation est exposée. Ils doutent, en revanche, que les employés soient conscients du problème. Ainsi, pour une majorité de DSI (53 %), le manque de connaissances des salariés en la matière figure au top 3 des risques qui planent sur les entreprises. Toutefois, c'est le vol de données qui inquiète le plus les DSI (63 %), et devance l'utilisation frauduleuse des données exfiltrées (52 %).

Retrouver la confiance en interne

Les attaques par déni de service, le piratage informatique, les virus, les malwares et autres ransomwares sont bien connus des DSI. Ils savent aussi que l'origine des menaces peut être interne à l'entreprise. Un initié peut tirer profit d'une faille, un collaborateur mobile adepte du BYOD (*Bring Your own Device*) peut ne pas respecter les règles de sécurité de l'entreprise. Or, 79 % d'entre elles autorisent leurs collaborateurs à accéder aux données internes depuis les terminaux personnels…

Pour protéger les données de l'entreprise sur les appareils mobiles appartenant aux salariés, le déploiement de solutions de sécurité dédiées est plébiscité (par 62 % des DSI). Suivent : la mise en place d'un stytème d'authentification et d'autorisation d'accès au réseau d'entreprise (48 %), ainsi que la formation des collaborateurs (47 %). La signature d'une charte d'utilisation des données par les collaborateurs arrive ensuite (31 %). Un quart des DSI recommandent l'interdiction pure et simple de l'accès aux données internes à l'organisation depuis un terminal personnel.

Impliquer les fournisseurs

La faille peut également venir de fournisseurs, dont des PME qui n'ont pas les moyens de grands groupes. Pour mieux protéger les données échangées, les systèmes et les réseaux de leur entreprise, 69 % des DSI souhaitent un renforcement des mesures de sécurité mobile, 50 % une meilleure gestion des menaces avancées persistantes. Ces deux options devancent la renforcement de la sécurité dans le Cloud (39 %), l'externalisation (38 %) et l'authentification multi-facteurs (31 %). Quant à la vérification renforcée des sociétés qui accèdent aux données, elle a moins d'adeptes (22 %).

Gérer les compétences

73 % des DSI pensent qu'ils seront confrontés à un plus grand nombre de menaces de sécurité dans les cinq ans à venir. Or, selon le cabinet Robert Half, les menaces informatiques ont évolué plus rapidement que les compétences, entraînant une pénurie de spécialistes en sécurité informatique, des analystes aux RSSI (responsables de la sécurité des systèmes d'information).

« Il faut des compétences techniques extrêmement pointues, cela va de soi, mais la capacité à s'exprimer clairement sur la cybersécurité, dans un langage compréhensible par les dirigeants et les collaborateurs d'autres départements que la DSI est cruciale, a commenté Fabrice Coudray, directeur de Robert Half Technologie France. *Cela permet de sensibiliser l'entreprise à la sécurité et d'améliorer la réputation de la DSI »*, qui devient un véritable *« business partner »* créateur de valeur pour l'entreprise.

Lire aussi :

Les DSI sommés de mieux mesurer ce qu'ils dépensent

Les voyageurs d'affaires ignorent les risques du WiFi public

Fuite de données : un coût moyen de 4 millions de dollars

crédit photo © Tamidichi / Shutterstock.com