Sécurité : pourquoi le poste de travail des administrateurs IT est trop exposé

Pour le fondateur et président du directoire de Systancia, Christophe Corne, « la sécurité du système d'information (SI) implique la séparation étanche entre tâches stratégiques sur le SI et tout le reste, actions professionnelles et personnelles incluses ». La mutualisation des infrastructures d'administration informatique avec celles utilisées pour les applications métier exposant davantage l'organisation aux menaces cyber.

Pourtant, cette mutualisation est encore trop souvent utilisée en France. C'est l'un des enseignements d'un sondage promu par Systancia.

L'enquête a été réalisée fin août par OpinionWay auprès de 305 directeurs des systèmes d'information (DSI) d'entreprises d'au moins 100 salariés. Des PME, des entreprises de taille intermédiaire (ETI) et des grandes entreprises sont donc concernées.

Premier constat : 29% des DSI d'entreprises de plus de 1 000 salariés déclarent que leur organisation n'emploie pas de responsable de la sécurité des systèmes d'information (RSSI). Ce taux atteint même 36% pour l'ensemble de l'échantillon.

Malgré tout, une majorité a un administrateur en charge de la sécurité du SI. Celui-ci dispose, entre autres, d'accès privilégiés et étendus au SI de l'organisation qui l'emploie.

Pourtant, 72% des entreprises concernées par l'enquête n'ont pas d'infrastructure dédiée aux seules opérations d'administration IT. Et ce malgré les recommandations en ce sens de l'Agence nationale de la sécurité des systèmes d'information (ANSSI). 28% l'ont.

De même, parmi les 64% de DSI déclarant s'appuyer sur un administrateur, 43% seulement indiquent qu'il dispose de postes de travail/serveurs séparés : l'un pour l'administration informatique, le deuxième pour d'autres applications professionnelles et personnelles.

Intelligence collective et artificielle

La séparation des environnements (administration IT d'un côté, applicatif métier de d'autre) n'est pas l'unique enjeu. La sensibilisation des équipes métiers aux bonnes pratiques et aux nouveaux usages en matière de sécurité informatique en est un autre.

Bonne nouvelle : la prise de conscience progresse (pour 87% des DSI interrogés). Mais 57% des répondants jugent que les salariés de leur organisation ne sont pas assez « formés » dans ce domaine pour contribuer à la sécurité du SI et reduire le risque de piratage.

Il reste que le risque peut également être réduit par l'utilisation de l'intelligence artificielle (IA). 67% des DSI interrogés le pensent. Mais 10% d'entre eux ne se prononcent pas.

Systancia, qui édite logiciels de sécurité des SI et de virtualisation, veut les convaincre.

(crédit photo © Shutterstock)